TLTA
TEXAS LAND TITLE ASSOCIATION

Provided courtesy of:

Capital Title℠
A Shaddock Company

AVOIDING AND RESPONDING TO WIRE FRAUD:

Tips for Real Estate Agents and Their Customers

1. **EDUCATE YOUR CLIENTS.** At the beginning of the transaction, real estate agents should have clients sign an acknowledgment that warns them about wire fraud. This acknowledgement should state that the agent will never provide wiring instructions – those instructions will always come from the title company. If the buyer receives a phone call, fax or email regarding wiring funds, they should not call back a number listed on the email or reply back to the email; instead, they should call a previously validated phone number to verify the funding information. The reason for this extra security: criminals can easily spoof or fake the email addresses and can send fraudulent emails pretending to be the real estate agent, title company and/or lender, including an identical-looking signature block in their email – but with a new phone number. A criminal pretending to be a real estate agent/title company/lender is prepared to answer that number. This is why clients should never call unverified phone numbers in emails or reply to those emails. A good practice for real estate agents is to make sure their clients have accurate contact information for everyone involved at the beginning of the transaction.

2. **NEVER EMAIL TITLE COMPANY WIRE INSTRUCTIONS.** While it's common practice for real estate agents to communicate frequently with their clients by phone and email to ensure all information is communicated in a timely manner and to maintain a strong business relationship, real estate agents should never be involved with sending or communicating title company wire instructions. To help reduce the risk of wire fraud, the client needs to understand that wire instructions will only be delivered to them by the title company.

3. **LAST-MINUTE WIRING CHANGES ARE OFTEN FRAUDULENT.** Real estate agents should understand that any deviation from the initial wiring instruction is presumed fraudulent until proven otherwise. Title company employees will proceed with great caution when there is a last-minute change and must verify the change is not fraudulent. Sellers and borrowers receiving proceeds do not normally change wiring instructions at the last minute. Any changes must be confirmed by phone with a highly trusted contact phone number or, better yet, in person.

4. **CASHIER'S CHECKS.** A cashier's check is an excellent option for avoiding wire fraud. The title company can verify checks with the bank prior to funding.

5. **TWO-FACTOR AUTHENTICATION AND STRONG PASSWORDS.** All parties involved in the real estate transaction can reduce their risk by enabling two-factor authentication on as many online sites as possible, especially public domain email systems such as Yahoo and Gmail (though all email involving nonpublic, private and confidential client information should be sent only through secure email systems). Also, agents should require use of strong passwords

(minimum of 12 characters), require periodic password changes and implement lockouts. Unique passwords should be used for each application/system requiring a password.

6. **CYBER PROTECTIONS.** Some cyber fraud occurs because of human error, but some can be prevented with the right security. In addition to educating their staff and their customers about safe business practices, agents should implement industry-standard and recommended IT security protections for their computing environment (email, servers, network, applications) including but not limited to: 1) performing an annual (or semi, quarterly or continuous) security assessment, 2) implementing solutions that block spam before the user needs to decide if it's fake or not, 3) implementing strong password controls, 4) implementing and maintaining advanced endpoint threat protection solutions, 5) implementing multi-factor authentication for all applications including email, 6) implementing a process that insures all systems (operating, applications, etc.) have timely installation of security patches, 7) implementing a full-featured firewall with the ability to block unnecessary international traffic, 8) whenever possible, encrypting files at rest, in motion (think email) and especially on mobile devices, 9) implementing an ongoing training program that teaches and tests employees to avoid clicking on suspicious links or opening suspicious documents that may contain malware, 10) implementing a process that ensures multiple offsite backups of data are performed and tested to confirm backups are valid, and 11) avoiding the use of public access WiFi or free charging stations and utilizing VPN when using WiFi.

7. **CYBER AND WIRE FRAUD INSURANCE.** Agents should obtain insurance that will protect against loss due to wire fraud.

8. **WIRE FRAUD RESPONSE PLAN.** Companies should have written policies and procedures in place for responding to a wire fraud incident, and all employees should be trained on them. If funds are diverted, company employees must already know who is to be alerted upon discovery, what tasks they are responsible for performing and how to contact the banks involved (both the initiating and receiving banks), law enforcement, legal counsel and (if necessary) public relations. Any chance to recover diverted funds diminishes rapidly with the passage of time, so written policies and training on how to react are crucial.

WHEN FRAUD HAPPENS:

If you suspect a fraud is underway or has happened, act immediately! Contact your management team and provide all the details of the suspected fraud. The bank and FBI need to be contacted immediately among other steps that should be taken. All cyber crime incidents should be reported to the FBI's Internet Crime Complaint Center (IC3) at: www.ic3.gov/default.aspx.

SOURCES:

- Wire Fraud Email Template From NAR: www.nar.realtor/law-and-ethics/wire-fraud-email-notice-template
- Wire Fraud Alert From NAR: speakingofrealestate.blogs.realtor.org/2015/05/19/alert-wire-fraudsters-targeting-real-estate-transactions/
- Wire Fraud Prevention From NAR: www.nar.realtor/real-estate-services-update/urgent-alert-sophisticated-email-scams-targeting-the-real-estate-industry
- Wire Fraud Tips From Jessica Edgerton, NAR Associate Counsel: realtormag.realtor.org/for-brokers/network/article/2016/05/threat-wire-fraud-real
- FBI's Public Service Announcement Regarding Business Email Compromise: www.ic3.gov/media/2017/170504.aspx
- NAR Data Security: www.nar.realtor/law-and-ethics/nars-data-security-and-privacy-toolkit