TLTA
TEXAS LAND TITLE ASSOCIATION

AVOIDING AND RESPONDING TO WIRE FRAUD:

Tips for Title Insurance Companies and Their Customers

1. **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.

2. **CONSUMER EDUCATION.** At the start of a transaction, title companies should educate all parties about the growing risks of wire fraud. Buyers are especially at risk as they are often asked to wire funds to the title company as part of the closing. Title companies should call buyers to discuss wire fraud, explaining that only the title company (not the lender or real estate agent) will communicate wiring instructions. 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 title company should provide all parties up-to-date contact information at the beginning of the transaction and instruct buyers to use only that contact 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.

3. **CONTACTS LOG.** In addition, title companies should create a log of all approved parties' phone numbers and email addresses at the start of a transaction. This log should be readily available and referred to when calling or emailing anyone on the list. Phone numbers and email addresses provided later in the transaction (in new email signature lines, etc.) should never be used unless they have been verified by calling a validated phone number. Consider always forwarding, rather than replying, which will require typing in the email address/addresses – this can help avoid accidentally replying to a fraudulent email address.

4. **FUNDING PROCEDURES.** Prior to closing, the title company should determine how buyer's/seller's funds will be disbursed/received. Wire instructions provided by the seller prior to closing for seller's proceeds should be verified by seller at closing. Exercise extreme caution when asked to change wiring instructions after having received verified instructions. Last-minute changes are often fraudulent. Consider implementing a policy of only accepting post-closing changes that are done in person, and never via email or fax.

5. **MAIL-OUT CLOSINGS.** Title companies conducting a "mail-out" or "notary signing agent" closing should only accept wiring instructions that the seller completed in front of the notary signing agent, had them notarized and returned them with the package. A verified email should only be accepted when it comes with a confirming phone call.

6. **CENTRALIZED WIRE APPROVAL.** Title companies must implement centralized wire approval procedures that ensure each wire gets confirmed with a trusted phone number before being initiated/released, and that the wire is being sent to the exact name of the party on the transaction. All wire transfer requests should be reviewed and approved by someone trained and responsible for verifying wiring instructions. The person initiating the wire should include documentation showing how the wiring instructions were confirmed. If the verification is not included, the wire should not be initiated until full documentation is provided. If there are any red flags or concerns in the documentation, the wire should not be approved/initiated until those concerns are resolved.

7. **CONFIRMATION OF WIRE INSTRUCTIONS.** Title companies should confirm all wiring instructions by phone using a verified phone number. The phone number should be the same one provided at the start of the transaction or one that can be confidently confirmed as valid. Do not use a number provided by an unverified email or fax; these can be provided by criminals.

8. **CONFIRMING WIRE RECEIPT.** Confirm receipt of wired funds with the intended recipient using a verified phone number. Call the recipient immediately after funding to let them know they should receive a wire transfer, advising them to call to confirm the wire has been received. Follow up with them within a few hours if they do not call to confirm receipt.

9. **TARGETING LARGE DISBURSEMENTS.** Transactions that result in a large cash payment to a refinance borrower/seller are highly susceptible to attack. Criminals specifically target these types of disbursements. Title companies should educate their employees to be alert about this increased risk.

10. **FRIDAYS AND HOLIDAYS.** Title companies should be extra vigilant regarding disbursements from closing on Fridays and prior to holidays, as sophisticated criminals target these transactions.

11. **TWO-FACTOR AUTHENTICATION.** 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.

12. **SLOW DOWN.** Criminals often create false urgency to aid them in making title companies not follow procedures. Slow down and do not rush any procedures.

13. **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.

14. **CYBER AND WIRE FRAUD INSURANCE.** Title companies should obtain insurance that will protect against loss due to wire fraud.

15. **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:

- ALTA Wire Fraud Resources:
  www.tlta.com/TLTA/News_Articles/ALTA_Releases_Several_Resources_to_Help_Protect_Title_Companies_and_Customers_From_Wire_Fraud.aspx
- ALTA Notice About Phishing Emails:
  www.alta.org/news/news.cfm?20170801-Phishing-for-Wire-Transfers
- ALTA Wire Fraud Red Flags:
  www.alta.org/news/news.cfm?20170725-Red-Flags-to-Protect-Your-Company-Against-Wire-Fraud
- ALTA Sample Wire Fraud Warnings:
  www.alta.org/news/news.cfm?20170725-Sample-Wire-Fraud-Warnings-You-Can-Use
- FBI's Public Service Announcement Regarding Business Email Compromise:
  www.ic3.gov/media/2017/170504.aspx

This information is being provided by TLTA for reference purposes only and is not intended to represent a standard best practice or the only approach to any particular issue. This information should not be construed as legal or business advice from or on behalf of TLTA. Users should consult their own legal counsel if necessary to ensure that any policies adopted or actions taken meet the unique security requirements of their company.