WIRE FRAUD
PREVENTION BULLETIN

May 2025

***Wire Fraud** continues to result in significant losses when closing funds are diverted to an account created by criminal actors. In most cases this result can be easily prevented when simple precautions are taken by the attorneys involved in a transaction, their staffs, and their clients.*

This Bulletin will address the need to:

I. Always independently verify wire instructions prior to acting on them

II. Be aware of the cyber-criminal risks involved when receiving, relaying, or using information involving real estate closings

III. Understand the liability associated with sending funds to a fraudulent account

IV. Obtain insurance if you decide to wire funds

V. Consider using and sending checks rather than wiring funds, and

VI. Establish mandatory office procedures in order to keep information and communications secure

Continues on next page...

Real Estate Conveyancing and Wire Fraud

Overview:

The reality of losing money because of criminal activity can hit very close to home when it is your clients' money that is lost or it is your law firm that transfers the funds into the fraudulent account. This Bulletin discusses practices that are designed to protect you, your customers, and your clients from becoming a victim of wire fraud, and that should be part of an overall office procedure when representing parties in a real estate transaction or issuing a title insurance policy.

Wire fraud scams often share similar facts:

- Fraudsters posing as a legitimate business send an email containing a link or an attachment to someone involved in the transaction, urging the recipient to click on the link in order to retrieve some documents. When the recipient opens that embedded link, a login page appears requesting a username and password. **If the person provides that information, the fraudsters can now log in using those credentials and monitor that person's email traffic;**
- Fraudsters with access to a compromised account can also divert and answer legitimate incoming emails which may never be seen by the compromised party;
- At a critical point, the fraudsters send an email to an attorney or paralegal involved in the transaction with fraudulent wiring instructions;
- The fraudsters may then call or email the recipient of the fraudulent wire instructions to confirm receipt;
- **Making a fateful error, the recipient fails to independently verify the wire instructions.** Tricked into believing that confirmation has been made, the recipient wires the funds per the wire instructions into the fraudster's account; and,
- When the fraud is discovered, the wire cannot be reversed, resulting in the total loss of funds and causing both reputational and financial harm to the firm.

The following represents a minimum acceptable standard that an office should meet when the office will be transferring funds by wire and issuing a CATIC policy.

I. **Confirm and verify all wire instructions by initiating contact with the purported sender through an email or phone number that is already known to you, or find contact information for the sender's web site after conducting an online search or using another reliable source of information, such as a bar association or business directory.** Do not use the contact information in the email or the facsimile message you received containing the wiring instructions, as this email or facsimile could be fraudulent, even if it looks authentic;

II. **Do not rely on "receiving" a confirming phone call or email. Confirm the wiring instructions by initiating a reply to the caller directly using known contact information. Verify telephone numbers or email addresses using a reputable source, or search the firm or business name via the internet.** The fraudsters are aware that title insurance companies are requiring verbal confirmation of wires, and they are calling the attorneys or paralegals themselves attempting to provide the required confirmation. Caller IDs may even appear to be coming from a reputable source when they are not;

III. **As an alternative, utilize checks to make payments via overnight delivery to an address that you can independently verify;**

IV. **Guard against last-minute changes to payoff instructions or other directions involving funds.** For example, consider imposing a general rule against acting on any revision request received within two business days prior to the closing date and after the closing has taken place. Include a notice of that rule in any correspondence your firm sends out to other offices and clients regarding real estate transactions. Tell clients not to act on any last-minute communication requiring a change without first calling the office number on your card or website for verification.

If you realize that a wire has been sent to a fraudulent account:

Follow the ALTA Rapid Response Plan for Wire Fraud Incidents, in other words, *immediately:*

1. Report the fraudulent wire to the sending and receiving banks and try to STOP the transfer and recall the wire.
2. Report the fraudulent wire to the FBI, Secret Service and local law enforcement. See the entire Plan for the complete list of actions.
3. If CATIC is the underwriter of any title insurance policy issued or to be issued, advise the CATIC Claims Department of the situation immediately.
4. Until a computer specialist with forensic and security experience has completed a review and/or repair of any computers or computer networks, assume that the fraudsters are still monitoring all e-mail communications.

The following are some additional strategies for mitigating risk:

1. Review your malpractice and other insurance policies with your insurance agents and carriers. Purchase proper cyber and crime coverages with social engineering fraud/wire transfer protection included. **Cyber and crime coverages, without the social engineering fraud/wire transfer protection, may not cover losses resulting from these transactions.** Also read and understand the terms, provisions, limits, sub-limits and exclusions. There is a lot of variation.
2. From verifying wiring instructions for a single transaction to physically handling the disbursement of funds via wire, there are companies that offer a range of services designed to assist Agents in detecting and minimizing wire fraud. **Contact your CATIC Agent Services Representative if you would like to know more about available wire fraud prevention services.**

Continues on next page...

Regardless of the size of the firm, agency or company, everyone on staff is responsible for cybersecurity.

Once a breach occurs and fraudsters have access to confidential information, this can compromise the entire system. **Also remember that no matter how careful your firm may be, some other party with whom you or someone in your firm is communicating may have experienced a cybersecurity breach.** It is therefore very important for you and your entire staff to recognize these threats, and for your firm to have reasonable procedures in place to try to prevent wire fraud from harming your firm or your clients.

Best Practices:

1. **Verify and confirm the validity of any email before taking any action or providing any information in response.**
2. **Never open any attachment or link in an email, unless you are certain of the source and have confirmed that the email is valid.**
3. **Never share usernames and passwords.**
4. **Hover over all URLs.** Should you receive an email from Dropbox, ensure that the URL does, in fact, go to Dropbox and not some unaffiliated, random website.
5. **Create office policies and procedures for all staff to follow, including guidance on when it is appropriate to open any attachment, or click on any link, use of the internet, and social media activity concerns.** Provide education and training on these policies and procedures to your entire staff.
6. **Conduct cybersecurity awareness training on a regular cadence with your staff, as well as simulated phishing campaigns.**
   - Research has found that employees who undergo cybersecurity training are more capable at spotting phishing-related emails.
7. **Keep all software current and use updated antivirus protection and firewalls.**
8. **Use multi-factor authentication for logins.**
9. **Use strong passwords and change them regularly.** Do not use passwords for business that you use personally and do not use passwords for banking transactions that you use for other matters.
10. **Have an incident response plan in place.**
    - Nearly half of all companies reported recovering faster with an incident response plan in place after an event transpired.
11. **Perform routine backups of your data.**
12. **Implement spam filters.**
    - Spam filters allow companies to achieve granularity when it comes to limiting the amount of junk, phishing, malware., etc., that can come though their systems.
    - Add attachment filtering, inbound/outbound URL protections, etc.
13. **Enforce least privilege across your organization.**
    - This means that you only provide employees with the necessary access needed to do their jobs.
14. **Access bank websites by typing in the URL.** Do not rely on links sent to you.
15. **Do not access a bank website using public computers or public Wi-Fi networks.**
16. **Discuss with the banks the security measures you can have implemented to protect funds, such as Positive Pay and/or Reverse Positive Pay for accounts, restrictions on ACH matters, restrictions on international transactions, alerts pushed to you for activity on your accounts.**
17. **Hire and speak to a computer specialist if you have any questions or concerns.**