Strategies to Combat Wire Fraud

Multilayered Approach to Security Helps Combat Attacks *(cont'd)*

Why Wire Fraud is a Growing Concern

Real estate transactions are attractive targets for fraudsters due to the large sums of money involved. “Just one or two fraudulent transactions can result in a huge payday for cybercriminals,” Quintyne noted.

In addition, one in four title companies reported experiencing a seller impersonation attempt in 2023, according to a study conducted by ndp | analytics. When the next report comes out, it's expected this number increased in 2024.

Nikki Pfleger, executive vice president and specialty deposits relationship manager lead at Encore Bank, highlighted another reason real estate transactions are particularly vulnerable: consumer inexperience. “These scams work because buyers and sellers don’t always know what to expect,” she said. “They trust the professionals they’re working with, and fraudsters exploit that trust.”

Emerging Trends: Deepfake Technology and Seller Impersonation

A growing concern in real estate fraud is the use of deepfake technology, which allows criminals to manipulate audio and video to impersonate legitimate parties.

Quintyne highlights the 2025 Entrust Identity Fraud Report that showed a deepfake fraud attempt occurs every five minutes. “These scams are getting more sophisticated, making it harder for professionals to identify fake identities,” she added.

Fraudsters also exploit gaps in title verification processes to commit seller impersonation fraud, particularly in transactions involving vacant land or unencumbered properties.

“One of my clients recently caught a seller impersonation scam because of a simple discrepancy—the name on the seller’s email didn’t match how they signed legal documents,” Pfleger said. “That small detail led her to investigate further, and she ultimately prevented a fraudulent sale.”

These incidents highlight the critical need for increased vigilance and verification throughout the entire transaction process.

Best Practices to Prevent Wire Fraud

To effectively combat fraud, title professionals must take a multilayered approach to security, focusing on people, process and technology, Quintyne recommended.

1. Strengthening Employee Training and Consumer Awareness

People are the first line of defense against wire fraud. Continuous training helps employees recognize red flags and respond effectively to potential threats.

“Fraudsters rely on urgency to pressure employees into bypassing security measures,” Pfleger explained. “If a request seems rushed, that’s a red flag.”

According to an ALTA survey of title companies:

- 78% conduct employee training at least once a year.
- 62% provide training on a weekly, monthly or quarterly basis.

However, experts warn annual training is not enough. “Fraud tactics evolve rapidly,” Quintyne stressed. “Companies that implement frequent training sessions—whether monthly or quarterly—are more successful in stopping scams before they happen.”

In addition to training employees, consumer education is equally important. “Most scams can be avoided if consumers know to verify wire instructions directly with their title company,” Quintyne added.

To raise awareness, title companies should:

- Provide written warnings in emails and transaction documents.
- Encourage consumers to call a known number before wiring funds.
- Offer educational materials about common fraud tactics.

ALTA provides several **resources** to help title and settlement companies protect against wire fraud and to raise awareness about the threat with customers. Here are a few:

- **ALTA Outgoing Wire Preparation Checklist:** Companies can use this checklist as a best practice for verifying outgoing wire information.
- **ALTA Rapid Response Plan for Wire Fraud Incidents:** This documented process has been developed by the ALTA Information Security Committee.
- **Protect Your Money From Wire Fraud Schemes Video:** Buying and selling a home is an exciting time, but there can be pitfalls for unsuspecting consumers.
- **ALTA Wire Fraud Infographic:** This handout explains the steps a consumer should take to avoid becoming a victim of wire transfer fraud.

2. Implementing Rigorous Verification Processes

Verification procedures must be thorough and multi-layered to reduce the risk of fraud. Key steps include:

- Using secure communication portals instead of email to prevent business email compromise.
- Verifying identities early and throughout the transaction—not just before closing.
- Conducting call-back verifications using previously verified phone numbers, not numbers provided in emails.

Quintyne also suggested title and settlement companies maintain a Written Information Security Plan (WISP), which is now required in ALTA's Best Practices. They should also ensure vendors' security is consistent with their own company standards, periodically review system login activity and look for anomalies and suspicious behavior, keep systems updated with latest patches and maintain strong banking relationships.

A common red flag is an urgent request for wire changes. "Fraudsters want to create a sense of urgency to prevent verification," Pfleger noted. "They push for quick action because once the money is wired, it's gone."

Another dangerous type of transaction involves LLCs and other corporate structures:

- Independently verify corporate documents through official state websites.
- Scrutinize changes in ownership or management—sudden transfers may indicate fraud.
- Look for inconsistencies in naming conventions (e.g., "Company LLC" vs. "Company CO").

"A small detail like a missing letter or abbreviation can be the difference between catching a fraud attempt or losing thousands of dollars," Pfleger warned.

3. Leveraging Technology to Detect Fraud

Technology can strengthen fraud prevention efforts when used correctly. Title professionals should integrate:

Wire Fraud Detection Software

Modern fraud detection tools analyze multiple data points to flag suspicious activity. Features to look for include:

- Public record checks to verify ownership history.
- ID verification software that detects forged or manipulated documents.

- Transaction monitoring tools that identify unusual patterns.

"Technology is a powerful tool, but it's only as strong as the people using it," Pfleger emphasized. "Firms need to carefully evaluate their bank partners, and their software and cybersecurity vendors, and stay proactive in implementing new fraud prevention measures."

Multi-Factor Authentication (MFA) and Secure Portals

Secure communication channels prevent business email compromise by ensuring sensitive information isn't transmitted via unprotected emails. Many regulations require MFA. The latest iteration of **ALTA's Best Practices** now requires the use of MFA.

"Fraudsters will exploit any weak link," Pfleger cautioned. "Every organization should be using multi-factor authentication, password management protocols and encrypted communication tools."

The Role of Industry Collaboration

Stopping wire fraud requires cooperation between title companies, financial institutions and law enforcement agencies.

"The bad actors are sharing information," Quintyne noted. "That means we need to do the same. If an attempt happens, report it. The more data we share, the better we can protect ourselves.

ALTA urges companies to report fraud incidents to the FBI's Internet Crime Complaint Center (**IC3.gov**). Even if a fraud attempt is unsuccessful, reporting it helps law enforcement track trends and build cases against these criminals, Quintyne added.

Staying Ahead of the Fraudsters

As fraud tactics evolve, businesses must remain proactive, adaptable and collaborative in their defenses.

"Crime thrives in silence," Pfleger said. "It may feel embarrassing if your company experiences an attack, but hiding it only helps the fraudsters. The more we share and collaborate, the better we can protect our industry."

Quintyne emphasized that wire fraud isn't going away, but companies can stay ahead by continuously improving their security strategies.

"Fraud prevention isn't just about reacting—it's about preparing," she said. "Strengthen your people, processes and technology. The more layers of defense you have, the harder it becomes for criminals to succeed."

"By prioritizing employee training, consumer education, robust verification processes and advanced technology, title companies and escrow agents can significantly reduce the risk of wire fraud and protect their clients from devastating financial losses," Quintyne concluded.