PATTEN TITLE COMPANY

Understanding Real Estate WIRE FRAUD

Cybercrime has reached epidemic proportions, and real estate wire fraud is one of its most toxic strains. In its 2022 Congressional Report on Business Email Compromise and Real Estate Wire Fraud, the FBI deemed the category "one of the fastest-growing, most financially damaging internet-enabled crimes." Estimated cybercrime-related losses jumped from about $7 billion in 2021 to more than $10 billion in 2022, according to the FBI's most recent Internet Crime Report. Among the top crime types in the report was real estate wire fraud conducted using identity theft or data breach.

The good news is that despite the increasing threat of real estate wire fraud, it is preventable. When buying or selling your next property, it's important to understand real estate wire fraud, how it's orchestrated, and how Patten Title protects its partners and exceeds national cybersecurity standards.

WHAT IS REAL ESTATE WIRE FRAUD?

Wire fraud is any scheme developed to defraud someone through the Internet or other electronic communications.

Real estate wire fraud is sometimes called "mortgage wire fraud" because it frequently targets homebuyers during the mortgage process. Criminals prey on buyers by impersonating their real estate agents, lenders or title agents and duping buyers into transferring down payments or closing cash into the perpetrators' accounts.

Real estate wire fraud can leave buyers without the money they need at closing and jeopardize home sales. Individual losses vary but can range from about $10,000 to hundreds of thousands of dollars.

It can be both time-consuming and costly to try to recover the money lost to real estate wire fraud. Even if you start as soon as the fraud is detected, it's very difficult to recover any funds lost.

HOW REAL ESTATE WIRE FRAUD IS CONDUCTED

Cybercriminals monitor for email accounts and phone numbers linked to home sales, particularly those of buyers and any associated real estate agents, lenders, and title companies.

These criminals then deploy a complex phishing scam, often using bogus emails, phone numbers, and websites to impersonate a known and trusted party. The con may include attempts to trick buyers into providing additional personal information or clicking links that download malware or otherwise facilitate access to login and password data.

After hackers have sufficient access, they track emails or text messages for mortgage closing dates and instructions. They may then send a message from an email or text that seems like an authentic source and contains updated transfer details for the down payment or closing costs.

These messages often include personal facts buyers believe only they and the other involved parties would know. Buyers may even receive calls from phone numbers and stakeholders that seem valid in an approach known as "spoofing."

The ultimate goal is to provoke homebuyers to initiate a wire transfer for their down payment or closing costs into an account that seems legitimate but is controlled by a criminal. Effective cybercriminals then hastily move that money, sometimes transferring it through several subsequent accounts to prevent detection.

continued

THE HIGH COSTS OF REAL ESTATE WIRE FRAUD

First-time homebuyers are commonly victimized in real estate wire fraud because they lack experience with the subtleties of the closing process.

As a Fortune magazine report about mortgage wire fraud notes, this means criminals often prey on younger homebuyers. Millennial and GenZ homebuyers — those between ages 23 and 41 — currently comprise the largest homebuying group, and most are first-time buyers.

This age group is also adept with technology and prefers electronic communications and internet-based transactions. Millennials and those younger are also more receptive to digital banking.

According to the Fortune article, real estate wire fraud cost homebuyers more than $350 million in 2021, with many of the victims young, first-time buyers who lack strong financial safety nets. But the casualties of real estate wire fraud aren't always young.

A recent AARP feature about wire fraud in real estate details how cybercriminals exploit older, less tech-savvy homebuyers. Many homebuyers in their mid-50s and older haven't purchased a new home in decades and are unfamiliar with cybercrimes like mortgage wire fraud as well as how to protect themselves.

Nearly 14,000 people were victims of real estate wire fraud in 2020, according to a wire fraud bulletin by the National Association of Realtors®. In 2020, real estate wire fraud losses topped $213 million and had jumped nearly 400 percent in three years.

The costs continue to multiply. The wire fraud prevention and recovery firm CertifID identified $1.4 billion worth of suspected wire fraud attempts in 2022, according to its State of Wire Fraud analysis.

CYBERCRIME AND REAL ESTATE WIRE FRAUD IN TEXAS

Texas consistently ranks among the top 10 states for both the number of cybercrime victims and the amount of cybercrime losses, including those associated with real estate wire fraud.

Texas followed only California and Florida in the total number of cybercrime victims in 2022, with more than 38,500, according to the FBI's Internet Crime Report. Texas ranked fourth in cybercrime losses, estimated at $763 million in 2022.

Real estate wire fraud was among the top 15 forms of cybercrime both in Texas and nationally in 2022. It followed cybercrime approaches often used to commit mortgage wire fraud, including phishing, personal data breaches, identity theft and spoofing.

CertifID's State of Wire Fraud report indicates the average real estate wire fraud loss for consumer recovery cases was nearly $107,000 in 2022. Still, FBI research suggests losses are often higher in states with higher median incomes and home values, including Texas.

PREVENTING WIRE FRAUD IN REAL ESTATE

Cybercriminals like those who execute real estate wire fraud are best stopped before they can access personal data and funds; many vanish without a trace. Essential tips for preventing real estate wire fraud include:

more

1. **Be wary of fraudulent emails:** Scrutinize any electronic communication that appears to be from homebuying stakeholders like real estate professionals, mortgage providers and title companies. Watch for misspellings or variances in names, email addresses, and websites.
2. **Be suspicious of sudden changes:** It's unusual for those involved with mortgage closings to make mistakes regarding accounts for down payments and closing costs or to send last-minute updates for wire transfers.
3. **Call and confirm:** Verify any wire transfer instructions with a call to your real estate agent, your lender or your title agent before you transfer funds. Use only a phone number that you've validated.
4. **Authenticate the details with your bank:** Ask your bank to corroborate the recipient's account number, as well as their name and location, before sending a wire transfer.
5. **Communicate with the recipient:** When wiring funds for a down payment or closing, call the lender or title agent to alert them of the pending transfer and amount. If the transfer is not immediate, follow up to verify timely receipt.

For more information about real estate closing scams and how to shield yourself and your finances, visit the Coalition to Stop Real Estate Wire Fraud. If you believe you're a victim of real estate wire fraud, inform your bank and ask them to contact the institution where the transfer was sent; then notify the FBI's Internet Crime Complaint Center.

HOW PATTEN TITLE PROTECTS OUR PARTNERS FROM WIRE FRAUD

Patten Title is dedicated to safeguarding our clients and customers from real estate wire fraud. We consistently achieve a Microsoft Secure Score that exceeds national standards. We accomplish this through a proactive, multimodal approach to identity protection and wire fraud prevention.

Key elements of our wire fraud security strategy include:

- **Continuous Secure Score monitoring:** Many organizations evaluate their Secure Scores monthly or quarterly. However, Patten Title monitors its Secure Score daily with a third-party source and immediately responds to threats.
- **CertifID software:** Patten Title also utilizes CertifID, which integrates with other software popularly used in real estate transactions to augment fraud protection and detection; it can even administer efforts to recover lost funds due to fraud.
- **ZOCCAM funds transfers:** ZOCCAM is an app designed for secure funds transfers and allows buyers to efficiently make earnest money deposits while protecting their confidential data.

Although homebuyers comprise the bulk of real estate wire fraud victims, bad actors exploit sellers, agents, mortgage providers, title agents and escrow officers. Patten Title is committed to extending wire fraud protections to everyone involved in a real estate transaction.