Real Estate Wire Fraud: What You Need to Know

The Scale of the Problem

Real estate wire fraud remains one of the most common and costly cybercrimes in the U.S., especially during property closings where large sums of money transfer quickly and electronically. According to the FBI's 2024 Internet Crime Complaint Center (IC3) Report, Americans filed over 859,000 complaints, representing $16.6 billion in reported losses — a 24% increase from 2023.

Within those totals, Business Email Compromise (BEC) — the primary vehicle for real estate wire fraud — accounted for $2.77 billion in losses, making it one of the top three most financially damaging forms of cybercrime. In 2024 specifically, there were 9,359 real estate and rental fraud complaints resulting in losses exceeding $173.6 million. One in four Americans reports being a target of wire fraud during a real estate transaction.

How It Works

Most schemes follow a predictable pattern. First, criminals identify upcoming transactions through public records, hacked email accounts, or data breaches of real estate software. They learn the parties involved, closing dates, and approximate transaction amounts. Then scammers gain access to email accounts through phishing or malware and monitor conversations to learn transaction details and timing. At a strategic moment — typically a few days before closing — the scammer sends an email appearing to be from the title company or real estate agent.
The email appears authentic, incorporating correct logos, professional language, and accurate property details, and includes "updated" wire transfer instructions that redirect funds to the criminal's account.

Red flags include a sudden change in wire instructions (it's rare for any party to change banking information mid-transaction), emails demanding urgent action especially at the end of the month or before bank holidays, and outreach through multiple channels like texts and phone calls about the wire transfer.

Can Stolen Funds Be Recovered?

Recovery rates remain limited. The FBI's Recovery Asset Team reported that it successfully froze or recovered 66% of attempted stolen funds in 2024 using its Financial Fraud Kill Chain — but time is critical. Victims who report within hours stand the best chance of recovery.

DAVID SEGATTI
630-290-7691 | david@davidsegatti.com
Broker - REALTOR® | www.davidsegatti.com

ERA REAL ESTATE PARTNERS

3-16-26

How to Protect Yourself

- **Always verify by phone.** Call your title company or closing agent at a number you look up independently — never use a number from the email in question — before wiring any funds.
- **Never trust email alone for wire instructions.** If giving financial information online, make sure the site is secure (look for "https"), and type web addresses manually rather than clicking links.
- **Watch for spoofed emails.** Sometimes fraud comes from a legitimate-looking email address where a single character has been swapped — for example, replacing "m" with "rn" — which can be very hard to spot.
- **Report immediately if targeted.** If you suspect wire fraud, contact your title company, bank, and the FBI's IC3 at ic3.gov right away.

New Regulations in 2026

A new FinCEN rule taking effect in 2026 mandates detailed reporting on all-cash real estate transactions, requiring new documentation and coordination between brokers, title companies, and financial institutions. Brokers must now maintain detailed records of transaction participants, funding sources, and beneficial ownership information. This rule is aimed at combating money laundering but also adds a layer of oversight that may help curb fraud.

The bottom line: the single most effective defense is a quick phone call to verify wiring instructions before sending any money. No matter how legitimate an email looks, independently confirm before you wire.

DAVID SEGATTI
630-290-7691 | david@davidsegatti.com
Broker - REALTOR® | www.davidsegatti.com

ERA REAL ESTATE PARTNERS