



Protect the Deal.

Every closing moves money, identities and trust. Here is where criminals slip in, and the habits that keep them out.

\$275M

lost to real estate
fraud in 2025

12,368

real estate victims reported
to the FBI

22,000+

complaints citing AI-
powered scams

58%

of stolen funds frozen
when reported fast

Where attackers strike

The inbox

Spoofed or hacked email from the "title company," lender or agent, timed right before closing.

The money

"Updated" wire instructions send earnest money or closing funds to a criminal's account.

Client data

IDs, bank statements and pre-approvals left in email, texts, phones and shared drives.

Six habits to start this week

1. **Call back before any money moves.** Use a number you already trust, never one from the email.
2. **Tell clients on day one:** "We will never change wire instructions by email."
3. **Turn on MFA** for email, MLS, e-signature and transaction software.
4. **Send documents through secure portals**, not email attachments or texts.
5. **Agree a code word** with your broker and team to beat cloned voices.
6. **Clear client files** from your phone and downloads after closing.

Red flags

- Last-minute change to wire or payment details
- Urgency or secrecy: "the account is being audited, send today"
- A sender address one letter off from the real one
- A seller who will not meet in person or on video
- Vacant land or a rental listed for quick cash sale
- Mail rules or forwarding in your inbox you did not create

If money goes to the wrong place: the first hour

1. Bank. Client calls their bank now and asks for a wire recall.

2. Report. File at ic3.gov with full transaction details.

3. Notify. Broker, title company, lender and the local FBI field office.

4. Contain. Reset passwords, check mail rules, alert IT.

Report a concern to
[NAME · PHONE]

Broker fraud contact
[NAME · PHONE]

My one new habit
