CLTA California Land Title Association
SINCE 1907

HELP STOP WIRE FRAUD

CONSIDERATIONS FOR ESCROW COMPANIES ON THE FRONT LINE IN THE FIGHT AGAINST FRAUD

Fraudsters have increasingly sought to exploit real estate transactions for illicit financial gain, placing escrow companies on the front lines in the fight against wire fraud. Criminals use spoofed emails, false payment instructions, and social engineering to redirect transaction funds.

As important participants in real estate transactions, escrow companies can help stop fraud before funds are lost by recognizing warning signs and verifying instructions before they are transmitted or acted upon.

HOW FRAUD REACHES ESCROW

Fraudsters may:

- Compromise or mimic trusted email accounts
- Send revised wire instructions that appear legitimate
- Exploit urgency to pressure staff to bypass verification steps

WHAT'S AT RISK

Fraudulently redirected funds:

- Buyer funds, seller proceeds, loan funds, or payoff funds

Delays and disruptions:

- Closings may be delayed or disrupted during investigations

Liability Exposure:

- Potential financial, operational, legal, or reputational harm

KEY REMINDER

Always verify wire instructions and payment changes through a trusted process.

WARNING SIGNS

Key red flags to look for in wire fraud schemes

- Last-minute changes to wire instructions or payoff details
- Email addresses with subtle spelling or domain mistakes
- Requests to keep payment changes confidential

WAYS TO REDUCE RISK

Verify before you send:

- Never rely on email alone to confirm wire instructions or payment changes
- Obtain verbal confirmation using existing, trusted contact information already on file
- Use internal review or dual approval for outgoing wires
- Document the verification process and any changes to payment instructions

Specialized verification services:

Potential financial, operational, legal, or reputational harm

- A number of vendors now specialize in wire fraud prevention services, including **CertifID**, **Closinglock**, and **FundingShield**

Any provider should be carefully evaluated to determine whether its services, security practices, and terms meet your company's needs.

SUSPECT FRAUD? ACT FAST

1. Contact the sending and receiving financial institutions immediately.
2. Notify affected parties, law enforcement, and internal leadership.
3. Report the incident to the FBI Internet Crime Complaint Center (IC3): www.ic3.gov

Fidelity National Title

FNT-HSWF