The Growing Thread of Wire Fraud in Real Estate Transactions - What Buyers & Sellers Need to Know

November 27, 2025 - I received an email from my broker that every Realtor dreads. An outside escrow company suffered a breach of its trust account. Funds from multiple buyers were reportedly stolen in what's being described as a hack, and several closings across our firm were halted on the spot. Because there is no public information available yet and I have no interest in interfering with any investigation, I'm not naming the escrow company involved. What I can say is that the description in my broker's email lines up almost exactly with previous documented escrow-trust hacks, and those cases tell us a lot about the risks, the liabilities, and the path forward for both consumers and real estate professionals.

The scenario he described mirrors, almost point for point, what happened in the Fountain Valley Escrow (FVE) and Integrity Escrow (IE) breach investigated by the California Department of Financial Protection and Innovation. In that case, hackers gained access to the escrow trust account at City National Bank and initiated a series of fraudulent wires totaling more than $1.9 million. Only part of the money was ever recovered. A shortage of more than $480,000 remained in the trust account, leaving buyers in limbo while the escrow companies and insurers tried to figure out who was responsible for plugging the hole. Regulators later found that the escrow companies attempted to fix the shortfall by shifting funds between unrelated trust accounts - something that is strictly prohibited - and ultimately issued an order shutting the companies' operations down entirely.

What happened there is instructive because it demonstrates just how vulnerable these systems can be and how long recovery can take. Unlike bank failures, a cyber-theft of escrow trust funds is typically not covered by FDIC insurance. That leaves the escrow company's private fidelity or cyber insurance as the only path to reimbursement, and those policies do not always apply. In the FVE case, their fidelity insurer declined to cover the stolen funds because the policy only applied to employee theft, not external hacks. Other coverage paid for forensic investigation and legal guidance - but not the actual missing money. Months or even years can pass before clients know whether they'll be made whole.

The liability issues are real and potentially devastating. As homeowners, buyers, and sellers, most people assume that if money goes missing, the scammer is the obvious person to blame and that insurance will cover any loss. But that isn't necessarily the case and the law doesn't always see it that way.

An article from the ABA about an Arizona case, Mago v. Arizona Escrow & Financial Corp., shows just how much exposure escrow companies can face when something goes wrong. In that case, a phishing email impersonating the seller tricked the escrow agent into wiring funds to a fraudulent account. The scammer was never found. The buyer sued. And the jury assigned 100 percent of the fault to the escrow agent - not to the fraudster. The appellate court upheld the verdict, finding that even though state law required juries to consider the fault of all parties, they were not required to assign any share of fault to the scammer if the evidence supported placing full responsibility on the escrow agent.

The ABA article is based on Arizona law, and laws vary from state to state. But it's a canary in the coal mine. Courts are increasingly signaling that escrow companies - not clients - bear the burden of verifying the authenticity of wire instructions. When something goes wrong, it is often the escrow holder who is left holding the bag. And if the escrow company cannot or will not make the client whole, litigation becomes the client's only remaining option.

All of this underscores how important it is for buyers and sellers to know how their escrow company handles security. We talk a lot about "using a strong escrow company," but most people don't actually know what to ask. My broker laid out the proper procedures to use, and frankly, every escrow firm should be operating at this level or better - because once the money leaves a trust account, you can't just call the bank and reverse a wire. Among the safeguards he described: banking information is never shared through standard email, wires require multiple layers of approval including passcodes that change every few seconds, checks cannot be casually issued or cashed, and random daily audits are performed to ensure every penny is accounted for. It's tedious, and yes, sometimes the policies feel annoying - but they exist precisely to prevent the kinds of losses that ruined the transactions in the FVE/IE breach and in the Arizona case. And from the looks of it, this recent breach will do the same thing.

There's another issue most clients don't realize: the escrow company does not "belong" to the agent. The buyer and seller are the direct clients of the escrow holder. They have every right - and frankly, the obligation - to ask direct

questions about how wire instructions are verified, how accounts are monitored, who approves funds leaving trust, and whether the company carries cyber and fidelity insurance that covers external hacks. Buyers should call their escrow officer. Sellers should call their escrow officer. This is not something the Realtor should handle on their behalf. It's their money on the line.

The rise of AI-driven impersonation, real-time synthetic voice cloning, and ever-more-sophisticated phishing attempts means that wire-fraud attempts are only going to accelerate. It's not alarmist to say that escrow companies are now prime targets for cybercriminals. It's simply the reality of modern real estate.

What we can do - as professionals and as consumers - is adopt the mindset my broker put so plainly: measure ten times, cut once. Slow down. Verify independently. Never accept wiring instructions from email without a phone call to a known number. Never "rush a wire." Never let a party force you to use an escrow company whose security measures you cannot verify.

This latest breach is a warning, but it's also an opportunity. If it makes us more careful, more skeptical, and more proactive about protecting client funds, then maybe some good can still come out of it. The stakes are high enough that we can't afford to get casual. If your escrow company can't clearly explain how they protect your money, it's time to find one that can. As my broker put it, "Run!"
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS