



# Cyber Insurance and Wire Fraud in Real Estate



Cyber criminals have been targeting real estate funds. Wire fraud in real estate has been around for a while now, but with the rise of new AI tools, scams are increasingly sophisticated. It's a good time to review your cyber insurance to verify that it provides the protection you'll need if you ever have a claim.

## ATTACKS AGAINST THE REAL ESTATE INDUSTRY

Real estate transactions tend to involve large sums, so it's not surprising that criminals have targeted these transactions. Common attacks involve various social engineering and impersonation scams. Here are just a few of the many, many examples:

- + A couple lost \$32,430 to a scammer when they were tricked into wiring their down payment to a scammer. According to Business Insider,<sup>1</sup> the couple had been emailing with a person they thought was their real estate agent for weeks, but it was actually a scammer who had accessed the agent's email account and then made up a fake story about needing to send the money to the seller's attorney.
- + Another couple lost \$160,000 in a similar scam. According to NBC 4 News,<sup>2</sup> the scammer posed as the couple's escrow agent to trick them into wiring the funds.
- + A Silicon Valley executive lost nearly \$400,000 in real estate wire transfer scam. According to CNBC,<sup>3</sup> she received an email that appeared to be from her mortgage broker with directions to wire the funds. The email looked legitimate – it even appeared to be a response to previous email she'd sent asking about the final steps – so she didn't hesitate to make the transfer.

Buyers and sellers are often unfamiliar with these processes, and they may be in a hurry to finalize deals in a competitive housing market. When you add in the fact that many of these scams are highly convincing, with scammers infiltrating legitimate email accounts and sometimes carrying on conversations for weeks, it's no wonder that so many people are losing money.

Real estate firms are expected to be the experts ensuring that processes go smoothly, and that may be why they are frequently found liable when things go wrong. According to Housingwire,<sup>4</sup> research shows that real estate agents, brokers and title companies are increasingly being held accountable when their clients fall victim to wire fraud. Common allegations include negligence, breach of contract, breach of fiduciary duty and deceptive business practices.

## THE PROBLEM IS GETTING WORSE

New AI tools are making it even easier for scammers to carry out convincing real estate impersonation scams and wire transfer fraud. Criminals can now use generative AI tools to craft emails that sound professional and do not contain the grammar and spelling errors often associated with phishing emails. Criminals can also employ chatbots to carry out conversations with targets, making it possible to conduct a large number of scams simultaneously. AI can also facilitate phishing attacks designed to steal login credentials from real estate brokers so that scammers can access email accounts and carry out wire transfer scams.

Zscaler found a 60% increase in AI-drive phishing attacks.<sup>5</sup> It's getting scary out there.

- + Be extra cautious about clicking on links or responding to emails and text messages.
- + Keep your accounts secure with strong passwords that you change regularly and use multi-factor authentications. Also monitor your accounts for breaches.
- + Warn your clients about the rise in wire transfer and impersonation scams and tell them how they should verify it's you before responding to correspondence.
- + Implement a process to confirm fund transfers. such as confirming transactions over the phone, or in-person.
- + Verify that you have sufficient coverage in place. The rise in cybercrime has made appropriate cyber insurance increasingly important.



## DOES YOUR INSURANCE PROTECT AGAINST CYBER RISKS?

When assessing your cyber coverage, consider whether your limits are high enough and whether your exclusions are acceptable.

In addition to the regular limits, cyber policies may contain sub-limits for social engineering losses and diversion of third-party funds. These losses can be substantial, and real estate agents who regularly deal with high-value properties and cash purchases may have greater-than-average exposures. Unfortunately, many policies provide very low sub-limits, particularly for diversion of third-party funds. Make sure you'll have sufficient coverage if you're held liable for wire fraud targeting a client's money.

Call-back provisions are another area to watch. Many cyber insurers have implemented strict cybersecurity requirements that their policyholders must adhere to. If you experience a loss and it's discovered that you were not following these procedures, your claim could be denied.

# DO YOU KNOW WHAT TO DO?

If you or one of your clients loses money to a scam, or if you experience another type of cybersecurity incident, immediate action is needed to minimize the loss.

- + **Contact the financial institutions involved.** It is not always possible to recover funds, but in some cases, it is if you act quickly enough.
- + **Contact your insurer.** Your policy likely requires prompt reporting and your insurer may be able to provide resources and guidance to help you respond to the threat.
- + **Secure any compromised accounts.** Take immediate action to change passwords and prevent further attacks.
- + **File a police report and notify the FTC.** Even if the police cannot assist in recovering the lost funds, it's good to have an official report.
- + **Hire a forensic investigator.** A forensic investigator can determine how the breach occurred. This is important to ensure that there are no remaining vulnerabilities and to prevent future incidents.

**Do you have the cyber insurance you need? IMA can help you secure insurance for losses stemming from cyberattacks and wire fraud in real estate.**

## AUTHOR:



**BLAKE SCHELLENBERG**  
*Executive Vice President*

## SOURCES:

- 1 Lloyd, Alcynna. (2024, July 6). *A scammer conned us out of our \$32,430 down payment by email. We didn't realize it until 10 days later.* Business Insider. <https://www.businessinsider.com/millennials-lost-down-payment-to-real-estate-wire-fraud-scam-2024-7>
- 2 Johnson, Carolyn, and Roher, Christine. (2024, February 22). *Southern California couple lost \$160,000 in a rapidly-growing down payment scam.* KNBC Los Angeles. <https://www.nbclosangeles.com/investigations/down-payment-scam-real-estate-escrow-home-buying-scams/3345114/>
- 3 Son, Hugh. (2024, July 23). *A Silicon Valley executive had \$400,000 stolen by cybercriminals while buying a home. Here's her warning.* CNBC. <https://www.cnbc.com/2024/07/23/wire-fraud-in-real-estate-silicon-valley-executive-warning.html>
- 4 Han, Brooklee. (2024, June 23). *Real estate firms may be on the hook for wire fraud losses: CertifID.* Housingwire. <https://www.housingwire.com/articles/real-estate-firms-may-be-on-the-hook-for-wire-fraud-losses-certifid/>
- 5 Wodecki, Natalia. (2024, April 23). *Zscaler Research Finds 60% Increase in AI-Driven Phishing Attacks.* Zscaler. <https://ir.zscaler.com/news-releases/news-release-details/zscaler-research-finds-60-increase-ai-driven-phishing-attacks>

This material is for general information only and should not be considered as a substitute for legal, medical, tax and/or actuarial advice. Contact the appropriate professional counsel for such matters. These materials are not exhaustive and are subject to possible changes in applicable laws, rules, and regulations and their interpretations.

NPN 1316541 | IMA, Inc dba IMA Insurance Services | California Lic #0H64724

©IMA Financial Group, Inc. 2025

CT-TL-IMA-RE-031025

IMACORP.COM