Guarding the Deal: Exposure to Real Estate Fraud in 2025

Abbey Fargen Riley

Part of the job of an attorney has always been helping clients mitigate risk. For many years now, the risks within real estate transactions have gone beyond the contractual arrangement itself and included the risks of moving money and conveying property interests in a digital world. We have included warnings in bold red letters in our email signatures reminding clients of the dangers of wire fraud and other common threats. But as technology has continued to evolve, so too have the tools of bad actors and the exposure we face in our transactional practices. Real estate fraud in 2025 is diversifying and accelerating, fueled by AI, cybercrime and gaps in identity and process safeguards.

While residential fraud has dominated headlines and taken place in high volume, bad actors are also active in the high-value, lower-volume world of commercial real estate. From wire fraud schemes targeting escrow funds to AI-enhanced document forgery and fraudulent syndications, the tools of deception are more advanced than ever before, requiring more vigilance than ever.

Wire Fraud and Attacks Targeting Escrows

Every real estate transaction includes various email threads between various parties (clients and attorneys, title companies and lenders) to communicate details of the transaction, including, in many cases, wire instructions. Fraudsters can hack into transaction email threads to inject fraudulent wire or payoff instructions to scam accounts prior to closing. Email accounts can be hacked and accessed, or fake email accounts can be created using cloned or spoofed email domains.

Data released by the Federal Trade Commission in March 2025 based on reporting to Consumer Sentinel showed that consumers reported losing more than $12.5 billion to fraud in 2024, an increase of 25% over 2023. While the data showed that the number of instances of fraud being reported remained stable compared to 2023, the success rate improved dramatically year over year, with 38% of people reporting fraud in 2024 losing money, compared to only 27% of reporters in 2023. In other words, the bad actors are getting better at fraud.

Business email compromise schemes have been around for many years and are one of the most common forms of real estate transaction fraud in both residential and commercial transactions. In its 2024 State of Wire Fraud Report, CertifID, a wire fraud protection company, reported that first time homebuyers are three times more likely to fall prey to wire fraud than repeat buyers, with median losses ranging from $72,000 for buyers to $70,000 for sellers, and $257,000 for mortgage payoff scams. Despite this, many consumers have little or no knowledge of the risks of wire fraud before closing, with the same CertifID report indicating that 51% of all consumers were "somewhat" or "not aware" of wire fraud risks.

And beyond the threat to consumers, increasingly these attacks are targeting law firms, title companies and escrow agents involved in multimillion dollar deals, where bad actors may monitor deal communications for weeks waiting for the right moment to act.

Although the bad actors have been increasingly successful in recent years, there are targeted ways attorneys can remain vigilant. Other important tools in avoiding wire fraud include:

- using secured email portals for transfer of financial information,
- explicitly notifying clients in engagement letters and verbally that wire instructions will never be updated via email alone,
- requiring dual verification for all incoming and outgoing wire instructions, and
- training staff to identify red flags.

AI-Generated Forgeries

AI, machine learning and even PDF software is enabling the creation of convincingly forged authority and transaction documents including LLC operating agreements and corporate bylaws, tenant estoppels, certificates of good standing, letters of credit, titles, appraisals, notarial certificates and pro formas. Although it has always been possible to falsify documents, current technology enables fake buyers and sellers, as well as fraudu-

(Continued on next page)

(Continued from previous page)

lent developers, a greater threat than ever before. Phishing attacks, for example, are reported to have increased by an astonishing 4,151% since the public release of ChatGPT in late 2022, according to cyber security firm SlashNext in "The State of Phishing 2024."

Beyond the capabilities of AI, many transactions, large and small, no longer take place in the same room across a closing table. Instead, we exchange paper and electronic packages, often electronically signed and sometimes electronically notarized.

Some of the ways to reduce exposure to the risks posed by digital forgeries include insistence on direct verification of key deal documentation with the applicable party or platform, and verification of entity formation and good standing directly through state records rather than reliance on PDF certificates. Electronically signed or notarized documents should be delivered or verified through the signing platform and the identity of parties to the transaction should be authenticated through enhanced due diligence, especially for off-market or fast-moving deals.

Mortgage Fraud

In residential transactions, fraud rings have been known to use blends of real and fabricated data to obtain mortgages across multiple states. On a smaller scale, individual borrowers may use fake income documentation sourced from gig economy platforms. Commercial borrowers and sometimes third-party "consultants" are submitting false or inflated documentation to obtain bridge financing, construction loans or mezzanine debt. This includes inflated budgets and appraisals, falsified lien waivers, contractor invoices and draw requests.

Lenders often rely heavily on attorneys to certify lien positions, making law firms potential targets for fraud liability. To mitigate this risk, attorneys should require independent third-party inspections before issuing opinion letters or certifying draws. Flag mismatches between borrower representations and publicly available data such as permits, zoning and GIS information. Avoid over-reliance on borrower-provided spreadsheets and payment information and be careful to review the representations and certifications that you are making in your form documents.

Cyber Threats: Ransomware, Data Breaches and Third-Party Risks

Real estate entities such as law firms, title companies and the clients and vendors with whom we often work closely face additional risks from ransomware and phishing. Bad actors gain unauthorized access and hold data hostage or access and retain client information. Hackers exploit vulnerabilities in emails as well as vendor systems, threatening data integrity and access and costing impacted companies billions of dollars annually. Massive leaks containing property-owner data can expose clients to identity theft and fraud, and there are many points of vulnerability to consider. In one well-known cyber security incident that occurred in December 2023, the Real Estate Wealth Network's client data system was breached, leading to the exposure of more than 1.5 billion records of real estate ownership data. Beyond the vulnerability of client information and liability, impacted firms often lose access to their own systems at least on a temporary basis, and may have to pay to regain access. According to "The State of Ransomware 2024" report by cybersecurity firm Sophos, ransomware impacted 59% of respondents, and more than half now pay the ransom.

Although there is no one permanent solution to avoid ransomware and phishing, training employees, implementing appropriate agent and vendor cybersecurity protocols, conducting due diligence on all third-party vendors and partners, are critical. It is also important to educate clients on privacy safeguards and use additional caution with the storage and transmission of nonpublic and financial information. (Vishnevetsky, G. (2024, September 20). Cybersecurity Threats in the Real Estate Industry: Risks and Protective Measures. *VLTA Examiner Magazine*.)

Conclusion

Commercial real estate attorneys must operate with the mindset of both a dealmaker and a gatekeeper. In 2025, the sophistication of bad actors demands a more scientific approach to legal diligence. For attorneys, the challenge is not only to spot fraud, but also to adopt and enforce protocols that prevent it without sacrificing deal flow.

Building in-house cyber capabilities and security training, updating fraud checklists, and maintaining awareness and skepticism are now essential elements of legal practice in commercial real estate.

Abbey Fargen Riley is a member of Stoll Keenon Ogden PLLC practicing in its Bank Transactions/ Finance/ Real Estate practice group and is the Chair of the LBA's Real Estate Section. She works in SKO's Jeffersonville, IN (formerly Applegate Fifer Pulliam) and Louisville offices. ■