AI, Deepfakes and the New Face of Fraud in Real Estate *(cont'd)*

The Rise of Deepfakes in Real Estate

Deepfakes—AI-generated videos, voices, and images that mimic real people—have moved from novelty to serious threat. Scammers can now clone a person's voice with just 30 seconds of audio, making fraudulent phone calls sound eerily authentic. In one real-world example, a California couple lost $720,000 after receiving a fake Zoom call from what appeared to be their real estate attorney.

In 2024, a Florida title company narrowly avoided fraud when a "seller" agreed to a video call. The person on the screen appeared real—until the title agent asked her to raise her hand. She didn't move. It was a deepfake.

"If a seller only wants to connect by text or email, it could mean something is amiss," the report warns.

Inside the AI Fraud Toolkit

The paper breaks down several AI-powered tactics criminals are using:

- Voice Cloning & Synthetic Audio: Used to impersonate professionals, especially during high-pressure wire transfer scenarios. "It only takes a few seconds of audio from a previous phone call, a video shared online or a social media post to recreate your voice," Closinglock wrote.
- Synthetic Identity Fraud: Fake personas created using stolen or generated data to commit deed fraud and open financial accounts.
- Generative AI Phishing: AI can write smart, personalized phishing emails that are often indistinguishable from legitimate correspondence. Studies show AI-written phishing emails are 3x more likely to get clicks than those written by humans. In **recent headlines**, a West Virginia woman received what looked like a legitimate email from her title company, featuring detailed instructions on wiring funds for her upcoming property closing. She promptly sent $255,000 per the instructions.
- Recon Bots & Data Scraping: Bots harvest data from MLS, LinkedIn and public sources to create hyper-personalized scams. Closinglock recommends title company IT teams must learn to detect these attacks via CAPTCHAs and user behavior analysis, and prevent them through web application firewalls and other measures.

Deepfake Video in Meetings: Though still rare, real estate video deepfakes are increasing in sophistication. In one example, the president of Florida Title and Trust encountered an AI-generated video impersonated a woman who was masquerading as a buyer. However, this particular deepfake video was not quite sleek and slick enough to fool a savvy viewer. That does not mean, however, that it won't happen again. Closinglock warns that as technology gets more sophisticated, deepfake video impersonators in meetings will be harder to detect. This is yet another trend to be aware of when you conduct meetings or transactions where information needs to remain private, such as real estate closings and wire transfers.

Why Real Estate Is Especially Vulnerable

Real estate transactions are prime targets for AI fraud because they combine:

- High-value financial transfers: Cyber criminals are savvy in recognizing that this can be the time and place to strike.
- Emotional, fast-paced timelines: Not every buyer is thinking straight when it comes to a suspicious email or text the day before the expected closing they've dreamed of for months or years.
- Widespread use of unsecured email and phone communication without additional authentication layers: Title companies should be using two-factor authentication.
- Publicly available data: This makes it easy for scammers to find property deeds, tax records, and upcoming sales that they can use to create realistic deepfakes.

In 2024, a Texas woman confessed to participating in a multi-part fraudulent real estate scheme with falsified lien payoff statements, falsified warranty deeds, and falsified emails to lenders, buyers, and title companies. While working for a trust company in McAllen, Texas, the fraudster used fake information for closings. Her duplicity resulted in losses of more than $350,000 for her title company. Even though the authorities caught the perpetrator, she still cost her clients and company dearly.

How Title Professionals Can Fight Back

The good news? There are smart, actionable steps professionals can take:

- Upgrade Identity Verification: Move beyond static IDs and use biometric or non-public data authentication.
- Standardize Communication Protocols: Never send wire instructions via email; always use secure portals.
- Vet Your Tech Vendors: Ask how they detect deepfakes, prevent spoofed calls, and use AI to enhance—not compromise—security.

- Follow ALTA Best Practices: These remain an essential foundation for compliance and protection.
- Train for Vigilance: Share real-life fraud cases in team training and reward fraud prevention wins.

“Building a fraud-resilient culture means encouraging employees to pause, ask questions, and speak up,” the report advises.

The Cultural and Legal Blind Spots

Regulations are lagging behind AI’s capabilities and liability is unclear when a deepfake tricks a title agent. Section 230 of the Communications Decency Act typically protects online platforms from liability for deepfakes, but this matter will continue to be debated. To navigate this, industry leaders must advocate for clearer definitions of “reasonable care” in an AI era.

The Real Risk: Social Engineering

Perhaps the most dangerous part of AI fraud isn’t the tech—it’s how believable it is. These scams prey on trust, emotion, and urgency. The more realistic the impersonation, the more likely someone is to comply without question.

“AI makes scams faster, more believable, and painfully personal,” Closinglock writes.

Human Intelligence Is Still Our Best Defense

Technology may be advancing, but human awareness remains the strongest protection. When professionals are empowered to slow down, verify, and escalate red flags, fraud loses its edge.

“Trust is the foundation of real estate—and AI is testing its limits,” the report concludes. “Fortunately, humans combined with the support of the right technology remain the best defense against fraud.”

*Contact ALTA at 202-296-3671 or **communications@alta.org**.*