



HOME > NEWS + PUBLICATIONS > INDUSTRY NEWS

Industry News

From Email to Voice Clone: How AI Is Fueling a New Wave of Real Estate Fraud

September 17, 2026

Brian and Wendy VanDoeselaar thought they were days away from closing on their dream condominium near Grand Rapids, Mich. Instead, they lost more than \$66,000 to what experts believe was a sophisticated scam that combined a spoofed email with AI-powered voice cloning. After receiving an urgent message directing them to wire funds, Brian received a confirmation call from someone who sounded exactly like their loan officer. The couple wired the money. By the time they discovered the instructions were fraudulent, the funds had disappeared.

The case illustrates a troubling evolution in real estate fraud. Criminals are no longer relying solely on fake emails, forged documents or spoofed phone numbers. Increasingly, they are using artificial intelligence to imitate trusted voices, create convincing communications and establish credibility at critical moments in a transaction. What was once an emerging threat is rapidly becoming a commercialized criminal service.

Voice Cloning Goes Mainstream

According to **NordVPN's 2026 Consumer Cybersecurity Report**, commercial activity surrounding AI voice-cloning services on dark web forums and Telegram channels increased 7.4 times between January-July 2024 and January-July 2026. Researchers found that advertisements for voice-cloning tools and services increased 82% in 2025 and another 75% during the first seven months of 2026 alone.

Even more concerning, mentions of voice cloning appeared more frequently on criminal forums during the first seven months of 2026 than during all of 2025.

"Voice used to be the thing that proved you were talking to a real person. That is over, and most people have not adjusted yet," said Adrianus Warmenhoven, cybersecurity advisor at NordVPN. "The phone is still where the bank calls, where family calls, where anything urgent comes through. That trust is now something criminals can buy their way into cheaply."

For title professionals, that observation carries significant implications. For years, a phone call has often served as a secondary method of verification when something about a transaction appeared unusual. Voice cloning technology is increasingly undermining that assumption.

The Rise of Fraud-as-a-Service

The NordVPN research found that voice cloning is no longer being marketed as a standalone novelty. Instead, it is increasingly bundled into broader criminal toolkits that combine AI-generated voices with auto-dialers, phishing platforms, identity-theft services and social-engineering scripts.

Researchers identified products advertising cloned bank phone systems, AI-powered "banker bots," voice-enabled phishing panels and fraud platforms capable of creating digital twins of targeted individuals. Criminals can purchase tools designed to impersonate customer service representatives, financial institutions and other trusted parties during phone calls.

The technology is also becoming remarkably affordable. NordVPN found that some automated voice-fraud tools can be rented for as little as \$30 per week, while standalone voice-cloning software sells for approximately \$400 to \$500. The low cost places sophisticated impersonation capabilities within reach of criminals who may have lacked the technical expertise or resources to conduct such attacks only a few years ago.

While bank impersonation and interactive voice response (IVR) scams were among the most frequently discussed applications on criminal forums, the same tactics can easily be adapted to real estate transactions. A cloned voice that appears to belong to a lender, title professional, real estate agent or property owner can provide the credibility needed to convince victims to transfer funds or move forward with a fraudulent sale.

AI is Changing Seller Impersonation Fraud

The title industry is already seeing evidence of this shift. According to **ALTA's 2026 Seller Impersonation Fraud Study**, nearly 60% of title companies reported experiencing at least one seller impersonation fraud attempt during the previous year. More importantly, 58% of respondents reported that deepfake technology, including AI-generated voice and image manipulation, was at least somewhat common in fraud attempts. Those findings suggest that artificial intelligence is rapidly becoming part of the criminal toolkit.

Seller impersonation fraud traditionally relied on forged documents, stolen identities and fabricated communications. Voice cloning adds another layer of deception. Fraudsters can now use AI-generated voices to support fraudulent narratives, answer questions, reinforce trust and potentially overcome doubts that might have surfaced during a live conversation.

The technology is particularly dangerous when combined with other fraud indicators commonly seen in seller impersonation schemes, including vacant land, absentee owners, free-and-clear properties and estates involving recently deceased owners.

Title Companies Fight Back

As fraud tactics evolve, title companies are responding with increasingly layered defenses. ALTA's study found that 94% of title companies employ multiple fraud-prevention tools and verification methods to identify suspicious transactions. Firms reported using an average of more than five different safeguards, reflecting a growing recognition that no single solution can stop every fraud attempt. Identity verification platforms, multifactor authentication, independently verified contact information, approved notary networks and direct outreach to property owners all rank among the industry's most commonly used defenses.

Title professionals are also paying closer attention to behavioral warning signs. Sellers who refuse video calls, insist on using their own notary, communicate exclusively through email, push for unusually fast closings or avoid standard verification procedures may trigger additional scrutiny.

Those safeguards have become increasingly important as AI-generated communications become more convincing.

A phone call that once might have resolved concerns may now require additional validation. Rather than relying on a single conversation, title companies are increasingly cross-checking identities through multiple sources, validating ownership records, confirming contact information through independent channels and requiring additional authentication when circumstances warrant. The study found that firms reporting greater confidence in their ability to detect seller impersonation fraud generally employed a broader range of verification tools and layered defenses.

Trust Still Requires Verification

The VanDoeselaar case demonstrates how quickly criminals are adapting emerging technologies to exploit trust. The threat is no longer limited to a fraudster sending a convincing email or placing a deceptive phone call. Criminals are increasingly combining AI-generated voices with stolen identities, spoofed phone numbers, fraudulent websites and automated phishing campaigns to create comprehensive fraud ecosystems.

As artificial intelligence becomes cheaper, more accessible and increasingly integrated into criminal operations, protecting consumers and property rights will depend not on any single technology or verification method, but on the industry's ability to continually adapt to evolving threats.

"The use of spoofed communications, stolen personal information and emerging technologies such as deepfakes demonstrates how quickly these schemes are evolving," said Elizabeth Blosser, ALTA Chief Strategy, Communications and Innovation Officer. "While the tools used by criminals may change, the industry's commitment to verifying identities, validating ownership and protecting consumers remains constant."

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



American Land Title Association
601 Pennsylvania Avenue, NW
Suite 750, North Building
Washington, D.C. 20004

P. 202.296.3671 F. 202.223.5843
service@alta.org

[Contact Us](#)

[ALTA Policy Forms](#)

[Advertise](#)

[Join ALTA](#)