

When the Voice on the Phone Isn't Real: How Our Threat Landscape Changed in a Year

Description

Article by Genady Vishnevetsky

The Call That Sounded Right

This past March, a couple buying a condominium in West Michigan got a phone call from their mortgage lender. The number on the caller ID matched. The voice matched. The caller walked them through where things stood in the transaction and then mentioned, almost as an aside, that closing funds needed to come in early. Wiring instructions would follow.

On the morning of closing, the title company called to confirm the buyers were bringing a certified check. That was the moment everyone found out the money was already gone.

No lender was on that call. A cloned voice, a spoofed phone number, and a criminal who understood the transaction timeline better than the buyer did.

Nothing about that scheme is new. Criminals have been redirecting closing funds for more than a decade. What changed is that the buyer had no reasonable way to know. Last year in these pages I wrote about infostealers, the quiet malware that harvests credentials while you work. This year the story is bigger than credentials. It is about trust itself, and how cheaply it can now be manufactured.

What the Numbers Tell Us

The FBI's Internet Crime Complaint Center passed a grim milestone in 2025: more than one million complaints and \$20.9 billion in reported losses, a 26 percent jump in a single year. Our corner of that report deserves attention. Real estate fraud complaints climbed to 12,368, and reported losses reached \$275.1 million, up roughly 60 percent from the prior year. Business email compromise remained the most financially destructive threat to businesses, with \$3.04 billion in reported losses, and about 86 percent of that money moved by wire or ACH.

For the first time, IC3 broke out artificial intelligence as its own category: more than 22,000 complaints and \$893 million in losses. The FBI has also noted that most victims do not realize AI was involved at all, so treat that number as a floor, not a ceiling.

Industry-specific data tells the same story up close. In a survey of 802 title and escrow professionals published this summer, nearly 80 percent of firms reported a fraud attempt during the previous year, and 86 percent said phishing and business email compromise were where attacks originated. Encouragingly, about 90 percent of firms stopped every attempt, up from 80 percent the year before. Less encouragingly, only 14 percent of victimized firms recovered all of their stolen funds, down from

18.5 percent.

Recently, ALTA released its 2026 Critical Issues Study on seller impersonation fraud. The findings are stark: 59 percent of title firms experienced at least one seller impersonation attempt in the prior calendar year, more than double the 28 percent reported in 2024. Forty-five percent had seen an attempt within the previous 30 days.

Six Shifts Worth Understanding

1. AI did not invent new crimes. It removed the friction. Every scheme we are seeing existed five years ago. What generative tools changed is cost, speed, and quality. Three seconds of audio is now enough to produce a convincing voice clone. Flawless English, correct terminology, and an accurate signature block are no longer signs of legitimacy. Security firm CrowdStrike reported an 89 percent year-over-year increase in operations by AI-enabled adversaries. The barrier to entry did not just drop; it collapsed.

2. The telephone became an attack surface. For twenty years we trained people to scrutinize email. Criminals responded by moving to the channel we never questioned. CrowdStrike observed voice phishing intrusions double in the first half of 2026 compared with the second half of 2025. In the ALTA study, 87 percent of firms rated spoofed contact information as at least somewhat common, and 58 percent said the same about deepfake voice or image technology. A familiar voice on a familiar number is no longer evidence of anything.

3. Impersonation moved beyond the seller Vacant land remains the top target at 82 percent, followed by absentee-owned property at 72 percent, property owned free and clear at 68 percent, and property of recently deceased owners at 55 percent. Criminals read obituaries and recorded death certificates, then run a rehearsed play against heirs who are grieving and unfamiliar with the file. The same tradecraft is now appearing in borrower impersonation for cash-out refinances, and with trillions in tappable equity sitting in American homes, that pressure will only increase.

4. Your vendors are part of your attack surface. Verizon's 2026 Data Breach Investigations Report found that breaches involving a third party reached 48 percent of the total, a 60 percent increase in a single year. Our industry lived this in November 2025, when a cyberattack at SitusAMC, a real estate finance services provider, exposed data tied to hundreds of thousands of individuals and drew in some of the largest banks in the country. A proposed settlement now covers roughly 662,000 people. Small firms are not spared: a title and escrow company in Lewis County, Washington, was hit by a ransomware group over the 2025 holidays, with 50 gigabytes of files claimed. You can outsource a function. You cannot outsource the consequences.

5. Ransomware changed shape rather than volume. Ransomware appeared in 48 percent of breaches in the Verizon dataset, but 69 percent of victims refused to pay, and the median payment fell to about \$140,000. Extortion is shifting from encryption toward data theft and publication, which for a title agency means client Social Security numbers and closing files rather than a locked server. The most useful finding for our industry is this: 73 percent of ransomware victims had an infostealer infection or credential leak in the year beforehand, half within 95 days. Stolen credentials are the on-ramp. That is why the quiet malware I wrote about last year matters so much.

6. Patching fell behind. Exploitation of software vulnerabilities overtook stolen credentials as the leading way attackers get in, and only 26 percent of critical vulnerabilities were fully remediated in 2025, down from 38 percent the year before. Most title operations rely on a handful of vendors and a browser. Ask when those systems were last updated, and who is responsible for confirming it.

Practical Steps for Title and Settlement Professionals

The good news, and it is real, is that our industry catches most of this. ALTA found that 87 percent of detected fraud is caught during the clearance and curative process, and 94 percent of firms now use layered defenses, averaging 5.3 tools apiece. The work is in closing the remaining gap.

Verify out of band, using a number you already had. Never call back the number on the caller ID, in the email signature, or in the document. Use the number from your own file, from the original engagement, or from the county record. This single habit defeats both spoofed calls and cloned voices.

Give every client a code word. Establish a shared phrase at the opening of the file and use it to confirm any conversation about money. It costs nothing, requires no vendor and works against a perfect voice clone. Do the same internally for wire release approvals.

Take the money conversation off email entirely. Wire instructions should never travel by email, and clients should be told in writing, at the outset, that instructions will never change by email or phone. A secure portal that keeps transaction communication out of open inboxes removes the channel criminals rely on.

Verify identity early, not at the signing table. We will spend days on a title search and less than a minute looking at the person signing the deed. Move identity verification to the front of the transaction and layer it: government ID with credential analysis, live biometric confirmation and device and database checks. A photograph of a driver's license is no longer a control. Consider using commercial ID Verification services.

Treat curative review as a fraud control, not just a title function. It is where most attempts are caught. Document the red flags your team looks for, and make sure examiners know their findings are a security function as much as a title one.

Make your authentication phishing-resistant. Text message codes are better than nothing, but criminals now routinely defeat them. Move to passkeys or hardware keys for email and your production system, and train staff to spot device-code approval prompts they didn't initiate. Attackers have shifted hard toward abusing legitimate login flows rather than stealing passwords outright.

Put your vendors in writing. Maintain a list of every third party that touches client data, including the ones nobody thinks of: the scanning service, the marketing platform, the IT provider. Require multi-factor authentication, ask for a current security attestation, and insist on prompt breach notification in the contract. Know, before something happens, what data each vendor holds.

Watch for your own exposed credentials. Assume some staff passwords are already for sale. Force password changes and session invalidation after any suspected infection, not just a password reset, and keep work and personal devices separate.

Rehearse the first hour. If funds go out the door, the recovery window is measured in hours. Call the originating bank first and file at ic3.gov immediately. The FBI's Financial Fraud Kill Chain initiated 3,900 incidents in 2025 and froze \$679 million of \$1.16 billion in attempted theft, a 58 percent success rate that depends almost entirely on speed. Write the phone numbers down on paper. Practice the call.

Train on what people hear, not only what they read. Your annual phishing simulation no longer covers the threat. Add voice scenarios, urgency scenarios, and a standing instruction that no one is ever penalized for pausing a transaction to verify.

Closing Thought

Every one of these controls trades a small amount of convenience for a large amount of protection. That trade has never been more worth making. The criminals targeting our industry are patient, well-funded, and now equipped with tools that can reproduce a trusted voice for the price of a streaming subscription.

Our clients hand us the largest financial transaction of their lives and trust us to guard it. They cannot evaluate a cloned voice. We can build a process that does not depend on their ability to.

Sources referenced

- FBI Internet Crime Complaint Center, *2025 Internet Crime Report* (April 2026)
- American Land Title Association, *2026 Critical Issues Study: Seller Impersonation Fraud* (September 14, 2026)
- Qualia, *Wire Fraud Trends in Title & Escrow, 2026: An Ever-Evolving Threat* (July 2026)
- Verizon, *2026 Data Breach Investigations Report* (May 2026)
- CrowdStrike, *2026 Global Threat Report* (February 2026) and *2026 Threat Hunting Report* (August 2026)
- HousingWire reporting on the ALTA study and on the SitusAMC incident;
- National Mortgage News reporting on the SitusAMC settlement

**Genady Vishnevetsky**

Genady Vishnevetsky serves as Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building successful security programs and developing the defense against emerging threats, Vishnevetsky leads security, governance, and compliance programs for global enterprises. Genady holds the following cybersecurity and risk management certifications â?? Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified in Risk and Information Systems Control (CRISK).

Category

1. Cybersecurity

Date Created

2026/09/30
Author
vltaexaminer

VLTA Examiner