Shumaker

JUNE 12, 2026 | PUBLICATION

Client Alert: Why Your Next "Urgent Call from the CEO" Might Be Synthetic and What to Do About It

In past years, wire fraud schemes relied on spoofed emails and compromised inboxes. Today, attackers are skipping the inbox entirely. Using generative AI, they can clone a voice, mimic tone and cadence, and place a call that sounds convincingly like your CEO, CFO, or trusted vendor.

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

This is no longer theoretical. The Federal Bureau of Investigation (FBI) has warned that criminals are increasingly using artificial intelligence (AI)-generated audio deepfakes in "vishing" (voice phishing) campaigns to pressure employees into transferring funds, resetting credentials, or disclosing sensitive information. According to Deloitte's Center for Financial Services, deepfake fraud losses reached $12.3 billion in 2023 and are projected to climb to $40 billion in the United States by 2027. What used to be a suspicious email is now a real-time conversation, and that changes the risk calculus for every organization.

What Has Changed and Why It Matters

Deepfake voice fraud is effective because it exploits human trust, urgency, and authority.

The old model involved phishing emails with suspicious grammar or links, giving targets time to pause and verify. The new model involves live phone calls or voicemails using a familiar voice—an executive, vendor, or IT help desk representative—combined with pressure to act immediately ("I'm boarding a flight—send this now").

The result: controls that rely on "spotting something off" are failing. Even sophisticated employees can be deceived when the request sounds authentic and urgent. A recent survey by cybersecurity company McAfee found that one in 10 Americans have now experienced a voice clone scam, and approximately 53 percent say they share their voice online at least once a week. According to Ben Colman, CEO of deepfake detection company Reality Defender, voice cloning technology has improved so rapidly that "even the PhDs on my team with their eyes can't tell the difference."

How These Attacks Actually Play Out

Most deepfake voice incidents follow a predictable pattern.

Reconnaissance

- Attackers gather public recordings such as earnings calls, podcasts, and social media videos. They research organizational charts, reporting lines, vendor relationships, and payment processes.

Voice Cloning

- Using widely available AI tools, attackers generate a synthetic voice that mimics a target's accent, cadence, speech patterns, and emotional tone. As Colman explains, creating a convincing voice clone now requires only three to five seconds of audio: "If I wanted to make a deepfake of you, I would simply go on Google, look up your name, I'd find a photo of you, perhaps on social media or LinkedIn, and then I would find audio of you."

Real-Time Engagement

- Attackers place a call or leave a voicemail with urgent requests such as "This is [CEO name]—I need you to process a wire immediately" or "I'm with a client, can't talk long—handle this discreetly."

Bypassing Controls

- They target vulnerable points, including treasury or accounts payable teams, executive assistants, and IT help desks (for password resets or multi-factor authentication (MFA) bypass).

Rapid Monetization.

- Funds are transferred or credentials are reset…often within minutes.

The threat is not limited to executives or public figures. Everyday individuals and small business owners are increasingly targeted as the technology becomes more accessible. In one example, Brewster County, Texas, Sheriff Ronnie Dodson discovered that someone had taken old YouTube videos of him and created a viral AI deepfake video using his real voice to endorse a health supplement.

Why This Is an Executive-Level Risk

This is not just an IT or security issue; it directly implicates multiple business functions. Finance and Treasury are exposed to wire transfers and payment fraud. Legal and Compliance face potential failures of internal controls and governance. HR and IT must address identity verification and access resets. Executive Leadership faces impersonation and reputational risk.

More importantly, these attacks weaponize leadership identity. Your voice, your authority, and your urgency become the attack vector.

Where Organizations Are Most Vulnerable

Across industries, the same gaps appear:

1. Overreliance on Voice-Based Trust – Employees assume that if it sounds like their boss, it must be real. This is particularly dangerous given Colman's observation: "In a world where you've been told for the

last decade that your voice is your password and now anyone can recreate any voice."
2. Weak Callback Protocols – Many organizations lack standardized processes to verify high-risk requests through independent channels.
3. Informal Payment Approval Workflows – A "just handle it quickly" culture overrides formal controls.
4. Help Desk Social Engineering Gaps – Attackers impersonate executives to reset passwords, add MFA devices, or unlock accounts.
5. Lack of Cross-Functional Coordination – Security, finance, and HR often operate in silos.

Practical Controls That Actually Work

The good news: this risk is highly controllable with the right discipline.

1. Mandatory Out-of-Band Verification – For any high-risk request involving wires, credential resets, or vendor changes, require verification through a second channel using pre-established contact methods only—not what the caller provides. There should be no exceptions for "urgent" or "confidential" requests. The key principle: trust the process, not the voice.
2. "No Voice-Only Authorization" Rule – Prohibit wire approvals via phone alone, password resets based solely on a call, and vendor payment changes without written and independently verified confirmation.
3. Treasury and Accounts Payable Hard Controls – Implement dual authorization for all wires, pre-approved vendor banking details, and cooling-off periods for new payment instructions.
4. Help Desk Identity Verification Protocols – Upgrade beyond knowledge-based questions. Require ticket-based workflows, manager approval for executive requests, and step-up authentication for sensitive changes. Security experts recommend asking questions that AI cannot easily guess, such as what someone had for dinner the night before.
5. Executive Communication Discipline – Leadership teams must avoid behaviors that create risk. This means no last-minute "urgent" payment requests outside process, no pressure to bypass controls, and a clear message that controls apply to executives too.
6. Targeted Training – Generic phishing training is insufficient. Train employees specifically on voice-based social engineering scenarios, "authority plus urgency" manipulation tactics, and exact steps to verify and escalate. Run simulations that include fake executive calls and help desk impersonation attempts.
7. Incident Response Readiness – If a deepfake attempt occurs, escalate immediately to legal and security; preserve call logs, recordings, and transaction data; and coordinate with financial institutions quickly. Speed matters—especially for wire recall.

The Regulatory Landscape: Federal and State Developments

Businesses should be aware that the regulatory environment around deepfakes and AI-generated content is rapidly evolving.

- Federal Action – At the federal level, Congress passed, and President Trump signed into law, the Take It Down Act in 2025, which makes it a crime to share intimate images without a person's consent, including deepfake videos. Notably, the law does not currently cover audio deepfakes. Additionally, Trump issued an executive order in December 2025 warning states against passing "onerous" AI legislation, establishing an AI Litigation Task Force within the U.S. Attorney General's Office to challenge state laws in conflict with federal standards, and threatening to withhold federal funding for rural high-speed internet access from non-compliant states.
- State Action – Despite federal pressure, states continue to legislate in this space. At least 26 states already have laws addressing AI-generated intimate depictions, and 46 states have some form of AI legislation covering areas from political advertising to pricing algorithms. Recent developments

include Missouri's House Bill 1887, which passed 145-3 in April 2026. The bill would make it a felony to share or threaten to share an AI-generated depiction of someone to harass, threaten, or harm them, with a maximum penalty of four years in prison—or ten years if the image depicts a minor. The bill also bars AI developers from advertising their products as capable of providing therapy or mental health diagnoses. As Missouri State Representative Bill Lucas observed, "We are living at a time when technology is evolving faster than our laws. Anybody with the basic tools can create and share harmful digital images that can destroy reputations and careers in seconds."
- Massachusetts has also taken action, issuing statewide guidance to schools following 2024 legislation signed by Governor Healey that made it a crime to create, possess, or share AI-generated intimate images of minors.
- Organizations should monitor both federal and state developments, as conflicting requirements may create compliance challenges.

Governance: What Boards and Executives Should Be Asking

- This is where leadership oversight becomes critical. Key questions for your board and executive team include:Do we have a no voice-only authorization policy?
- Are callback procedures documented and enforced?
- How do we verify executive identity in urgent scenarios?
- Are help desk controls aligned with modern social engineering threats?
- Have we tested this risk through tabletop exercises?

The Bottom Line

Deepfake voice fraud represents a shift from technical compromise to human compromise but with AI-enhanced realism.

The takeaway for business leaders is simple: if your controls assume that a familiar voice equals a trusted request, your organization is exposed.

The organizations that will manage this risk successfully are not the ones with the best AI tools—they are the ones with the strongest operational discipline: clear processes, enforced verification, executive alignment, and cross-functional coordination.

Because in 2026, cybersecurity is no longer just about systems. It is about who you trust and how you verify it.

For questions and more information regarding the risks of AI deepfakes, please contact Jade Davis or another member of Shumaker Technology, Data Privacy, Cybersecurity & AI Service Line.