# The New Face of Fraud: How Deepfakes Are Breaching Your Perimeter

by Tracey Nyholt, Presented by TechJutsu

## The Next Frontier of Social Engineering

Security professionals have spent the last decade hardening perimeters against phishing emails and credential stuffing. We have deployed firewalls, endpoint protection, and robust Multi-Factor Authentication (MFA) to lock down access. Attackers have been equally busy finding new ways around these defenses, and they are using the trust you have in your own employees against you.

That trust is being systematically exploited by impersonation, spoofing and social engineering with voice AI at a growing scale. The rise of generative AI has brought with it a dangerous new threat of advanced deepfakes that are increasingly available to the general public. These are much less clumsy than the cute but uncanny versions from the past. Today's audio deepfake technology can clone a CEO's voice with just a three-second audio sample. Video deepfakes are becoming no less impressive, able to generate real-time overlays of a subject, making that face on the other side of a Zoom call much less trustworthy.

With the breathtaking speed at which these technologies are developing, a growing security gap is becoming critical. When your employees can no longer trust what they see or hear, the traditional "human firewall" begins to crumble.

The financial sector has already seen the devastating potential of this technology. A finance worker at a multinational firm based in Hong Kong was tricked into

transferring $25 million in 2024. This worker was instructed to do so on a video conference call. The call appeared to be populated by the company's CFO and other colleagues, but almost everyone on that call was a deepfake persona generated in real-time (CNN 2024). This incident dispelled the notion that video presence equals proof of identity.

Voice cloning has added a dangerous new tool to vishing (voice phishing) scams. In one high-profile case, attackers used an AI clone of the CEO of a UK-based energy firm. They were able to successfully direct the transfer of €220,000 to a fraudulent supplier (WSJ 2019). By replicating the specific cadence and tone of a company's leadership, fraudsters can bypass the skepticism that would normally stop a suspicious call or email.

Emerging biometric hacking tools are making it increasingly difficult for organizations to distinguish between legitimate users and impostors.

These are not isolated events. The FBI's Internet Crime Complaint Center (IC3) has warned that emerging biometric hacking tools are making it increasingly difficult for organizations to distinguish between legitimate users and impostors (FBI 2023).

Most organizations still rely on sensory confirmation for sensitive requests. If we see a face on a webcam or hear a known voice on the phone, our brain defaults to trust. Deepfakes exploit this biological vulnerability. Traditional signals like caller ID and voice familiarity are no longer reliable.

Current verification methods are ill-equipped to handle this:

- **Video Calls:** Standard video conferencing tools do not natively verify that the video feed is authentic and not a synthetic overlay.
- **Voice Recognition:** As noted by the Federal Trade Commission, scammers can now clone voices for as little as a few dollars, rendering voice recognition software increasingly unreliable for high-security authentication (FTC 2023).
- **Knowledge-Based Verification:** Asking "security questions" is futile when the attacker has likely already scraped the answers from LinkedIn or the dark web.

We can no longer assume that your employees will be able to identify fraudulent callers. Technology is evolving faster than human perception, and it is a race we are destined to lose.

To put a stop to this new wave of AI-powered fraud, we must move beyond reliance on audio/visual cues and implement verifiable trust. We need to treat a video call or a phone request with the same "zero trust" scrutiny we apply to a network login attempt.

Organizations must rethink identity for the voice channel as a first-class security problem. Beyond a simple customer service utility, calls into your service desk are becoming a critical attack surface operating on an outdated model of implied trust. Telephones are the path of least resistance for attackers struggling with firewalls and endpoint protection. Phone-based requests for password changes or MFA resets must be considered on the same security tier as network access requests.

#### LEVERAGE OUT-OF-BAND AUTHENTICATION

NIST Digital Identity Guidelines (SP 800-63B) recommend the use of out-of-band (OOB) authenticators (NIST 2025). Using something outside of the voice or video call to authenticate a caller effectively eliminates the human factor that attackers are relying on with their deepfakes.

Tools that push a secure MFA challenge to the user's registered computer or mobile phone during a call can provide assurance that the caller is who they claim to be.

#### HARDEN THE HELP DESK

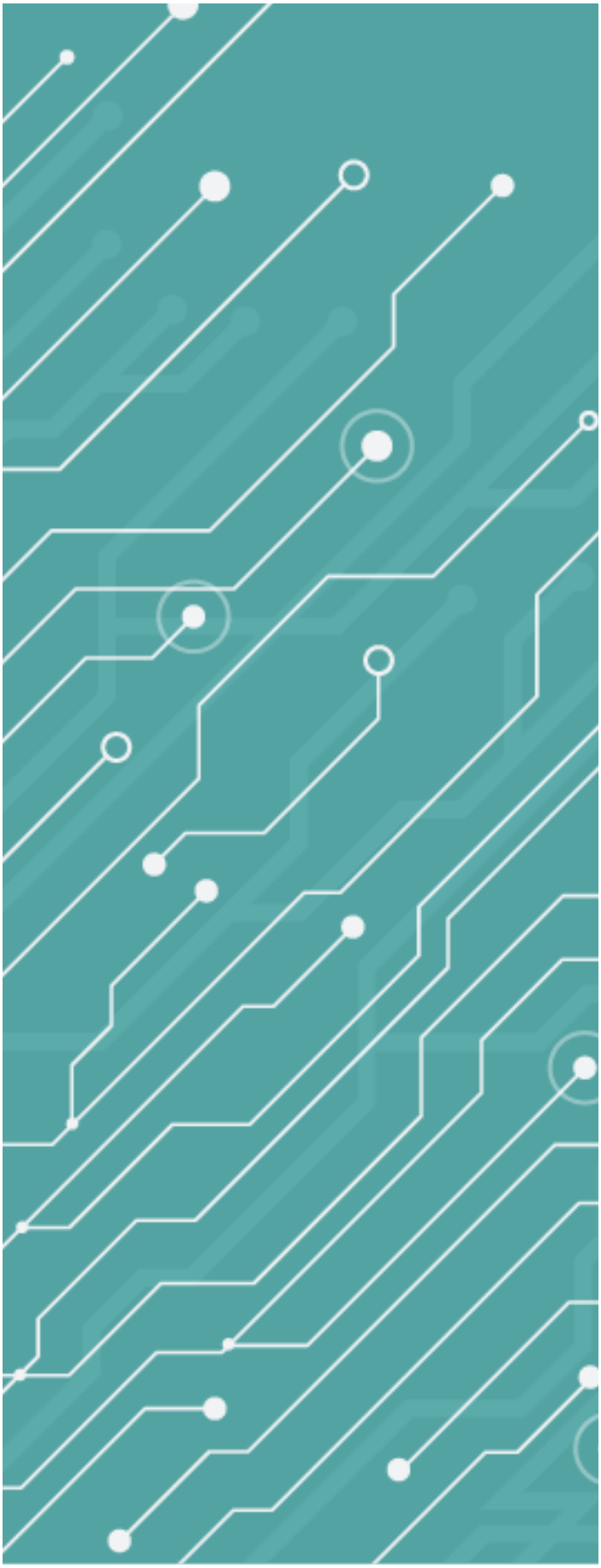
Integrate identity verification directly into your ITSM platform and call processes. Ensure that sensitive operations require secure user verification prior to making those changes.

Rather than rely on antiquated methods like easily guessed security questions, mandate that agents use phishing-resistant factors to authenticate callers. Empowering your service desk agents with tools that validate identities, you can ensure that they continue to both help and protect your organization.

By integrating robust, out-of-band authentication into our communication channels, we can inoculate our organizations against this new breed of fraud without crippling our operations. The technology to fake a face or clone a voice is here and becoming increasingly simple for even casual attackers to leverage. The counter-measures we deploy must not be cumbersome, however. We must ensure that digital identities are rigorously protected while simultaneously guaranteeing that the user experience remains as frictionless as possible. Security controls that frustrate users are security controls that are bypassed at every opportunity. Therefore, the goal is not just to build a higher wall, but to build a smarter gate. A gate that leverages the seamless, one-tap verification methods that employees already use in their everyday lives to deliver rigorous identity assurance in seconds. By balancing unyielding cryptographic security with intuitive, user-centric design, we can restore trust to our conversations without sacrificing the speed of business.

See end notes for this article's references.

Tracey Nyholt is the founder and CEO of TechJutsu, an IAM and cybersecurity firm specializing in closing security gaps in help desks and call centers. TechJutsu's Caller Verify solution allows call center agents to securely verify a caller's identity with the caller's own MFA factors.



# TRUST IS A TWO-WAY ROAD

## Secure the full circle of communication


### BUILT FOR REAL ATTACK SCENARIOS

Eliminate social engineering risks by stopping impersonation attempts

### REAL-TIME CALLER VERIFICATION

Verify every caller in under 10 seconds using secure MFA

### RAPID DEPLOYMENT

Go live in as little as one day with seamless ITSM integrations

Canadian-built cyber solutions

www.callerverify.com