GetReal

Deepfakes:

Your Agents Are Being Deceived Into Unknowingly Bypassing Security Controls

> *Agents can't rely on voice or video for identity verification anymore, and they shouldn't have to.*

What Customer Support Leaders Need to Know Now

Customer service agents are on the front line of a new threat: AI-generated voice and video that convincingly impersonate legitimate customers, enabling fraudsters to bypass authentication, manipulate account settings, and authorize fraudulent transactions. These attacks exploit the trust-based nature of customer support interactions, where agents are trained to be helpful and resolve issues quickly — precisely the instincts that deepfakes take advantage of.

When fraudsters use voice cloning to pass authentication checks or manipulate agents into resetting multi-factor authentication, changing contact details, or unlocking accounts, the contact center becomes the breach point. Traditional verification methods — voice recognition, knowledge-based questions, caller ID — are no longer sufficient. Deepfakes have invalidated the assumption that hearing a customer's voice or seeing them on video confirms their identity. This creates direct accountability for customer support leadership. When agents are deceived into facilitating fraud, the operational, financial, and reputational consequences fall on your function — even when agents followed established procedures.

Why This Is a Customer Support Leadership Issue

Customer service sits at a critical verification point: the live interaction where identity is confirmed before access is granted. Deepfakes exploit this moment by making fraudulent callers indistinguishable from legitimate customers.

- **Agent deception and fraud facilitation:** When agents cannot distinguish between real customers and AI-generated impersonators, they unknowingly authorize account takeovers, credential resets, and fraudulent transactions
- **Operational disruption and remediation costs:** Deepfake incidents trigger emergency response, account reviews, credential resets, and fraud investigations that consume team resources and disrupt normal operations
- **Customer trust and brand damage:** When customers learn their accounts were compromised through contact center interactions, trust in your service erodes and brand reputation suffers
- **Regulatory and compliance exposure:** Depending on the industry, inadequate identity verification in customer-facing operations may trigger regulatory scrutiny, particularly in financial services
- **Employee morale and confidence:** Agents who discover they were deceived by deepfakes experience stress, self-doubt, and reduced confidence in their ability to verify customers — impacting performance and retention

When contact centers operate on the assumption that voice and video provide reliable authentication, deepfakes turn agents into the weakest link.

What "Reasonable Preparedness" Looks Like

Leading customer support organizations are implementing layered verification and agent empowerment strategies to address deepfake threats:

- **Real-time deepfake detection and fraud alerts:** Deploy tools that analyze voice and video for synthetic indicators during live calls, flagging suspicious patterns (unusual locations, rapid successive calls, failed authentication) and providing agents with risk signals without adding friction to normal interactions
- **Multi-channel verification for high-risk actions:** Require verification through secure channels (in-app push notifications, biometric confirmation on registered devices) for account changes or credential resets — streamlined for legitimate customers while blocking impersonators
- **Enhanced authentication beyond voice:** Use behavioral biometrics, device fingerprinting, and context analysis that verify identity silently in the background — moving beyond knowledge-based questions that can be compromised
- **Agent training and empowerment:** Educate agents on deepfake indicators (urgency tactics, reluctance to use alternate verification) and create a culture where challenging suspicious requests is supported, even under customer pressure
- **Call recording for forensic review:** Maintain comprehensive recordings to identify verification gaps and support post-incident investigation

Real Consequences

Contact centers and customer support operations are already experiencing deepfake-enabled fraud at scale, with documented financial and operational impacts:

- **Voice phishing surged 442%** in 2024 as AI voice cloning enabled attackers to impersonate customers and bypass authentification. (Source)
- **Authorized Push Payment fraud surged** as deepfake impersonations manipulated victims into authorizing transfers, driving complaint volume and reimbursement demands. Call centers reported being overwhelmed by synthetic voice attacks targeting customer accounts. (Source)
- **More than one-third of consumers** across the U.S., U.K., Canada, and Europe encountered deepfake voice scams by early 2025, with losses frequently exceeding $6,000 per victim. (Source)
- **FBI warnings issued** about AI voice cloning used to impersonate senior officials and trusted contacts in phishing campaigns targeting customer service operations. (Source)

Bottom Line

Deepfakes have weaponized customer support interactions by making fraudulent callers indistinguishable from legitimate customers during live conversations. Voice and video no longer provide reliable identity verification, but contact center processes still depend on them.

Recommendation

Treat deepfake risk as a customer protection and operational security priority. Implement multi-layered verification beyond voice recognition, train agents to recognize and respond to impersonation attempts, and deploy real-time deepfake detection that provides identity-specific risk signals during interactions. A secure customer experience is a foundational component of brand trust.

About GetReal Security

GetReal Security is the cybersecurity leader specializing in the detection and mitigation of threats posed by malicious generative AI content including deepfakes and impersonation attacks. Its technology serves multinational corporations, financial institutions, media organizations, government agencies, and social media companies.

The company was incubated by Ballistic Ventures, the venture capital firm dedicated exclusively to funding and incubating entrepreneurs and innovations in cybersecurity, and Dr. Hany Farid, the preeminent expert in media forensics.

getrealsecurity.com