What Agentic AI Means for the Future of Fraud: The Deepfake Threat Playbook

Synthetic voice fraud is everywhere—saturating the threat landscape and accelerating across industries. This guide breaks down how deepfakes are reshaping fraud tactics, where legacy defenses are failing, and what organizations need to know to detect and respond at scale.

Key takeaways

- Synthetic voice fraud is no longer just a novelty—it's a strategic tool used by fraudsters to bypass both human intuition and automated defenses.
- Agentic AI systems are enabling fully autonomous attacks, allowing for fraud to occur at scale without human intervention.
- Organizations need modern, effective detection strategies that identify behavioral and technical anomalies in real time.

The rise of machine-led fraud

Deepfake technology has evolved rapidly and become deeply embedded in fraud operations. In 2024, **deepfake fraud grew by +1337% as compared to the previous year.**[1] It's persistent, dynamic, and growing more advanced by the day—and the pressure is mounting for organizations to keep up.

+1,337% increase
in 2024 in deepfake fraud from the previous year[1]

You're not talking to a person. You're talking to a machine.

According to Pindrop data, **1 in every 106 contact center calls** contains synthetic audio today.[1] These aren't just one-off voice clones or isolated social engineering attempts.

6.8x increase YoY
in non-live calls by the end of 2024[1]

We're now seeing the rise of **agentic AI**: systems that combine new forms of AI like large language models (LLMs) with traditional AI such as machine learning and enterprise automation to create autonomous 'AI agents'. These agents use AI-generated speech to imitate real people and can analyze data, set goals, and take actions to carry out fraud with decreasing human supervision.

This is the new reality of impersonation fraud at scale. It's not hypothetical. It's happening now.

+475% increase
in deepfake voice attacks in insurance and +149% in banking in 2024[1]

©2025 Pindrop®. All rights reserved.

Deepfake tactics that fool humans (+ some systems)

Modern voice cloning tools are dangerous because they don't just sound human—they feel human. They express emotion. They replicate tone, cadence, accent, and urgency in real time. They're used to impersonate executives, customers, employees, and even loved ones. And they're publicly available, continuously improving, and increasingly difficult to trace.

These are especially dangerous in contact centers, where agents rely on voice as a primary signal of identity. The human ear is poorly equipped to distinguish between synthetic and organic speech, especially under pressure.

Common deepfake fraud tactics

- **Real-time voice conversion** to mimic an individual's pitch, tone, and accent.
- **Emotion simulation**—urgency, empathy, and frustration are used to manipulate human targets.
- **Caller ID spoofing** that overrides metadata checks by faking trusted phone numbers.
- **Text-to-speech (TTS) and replay tools** to train systems on a target's speech patterns and trigger security loopholes.

Detection isn't optional—it's urgent

Deepfake fraud isn't just a threat; it's a financial liability. **Businesses have an average of $343,000 in deepfake fraud exposure in contact centers alone.**[1] Companies are facing hundreds of thousands of dollars in potential losses, and without real-time detection, fraudsters will continue to exploit security gaps.

Deepfakes now account for nearly 2% of all confirmed fraud cases,[1] and that number is rising quickly. Traditional methods of voice authentication are often not enough to withstand these new threats, and organizations must modernize their security systems to stay ahead.

$343K
average deepfake fraud exposure a business may face in their contact centers[1]

92%
of all businesses have experienced some financial losses due to deepfakes, says a Medius survey[2]

©2025 Pindrop®. All rights reserved.

Why legacy defenses are failing

Traditional identity verification methods weren't built for synthetic threats. Knowledge-based authentication (KBA), one-time passcodes (OTP), and even caller ID verification are often no longer sufficient. In a recent study, Pindrop found that **22% of OTP challenges are now being bypassed using synthetic speech.**[3]

Humans struggle to detect AI-generated voices, especially those that simulate emotion or urgency. What's more, voice analysis tools that aren't trained on synthetic threats are at risk.

Effective detection systems must:

- **Trace known synthetic voice sources**, such as popular text-to-speech (TTS) engines.
- **Analyze voice artifacts**—like unnatural timing, spectral distortions, and behavior patterns.
- **Cross-check video, audio, and movement** to flag inconsistencies across channels.

PRODUCT HIGHLIGHT

A good example of an effective liveness detection tool is Pindrop® Pulse, which is trained on over **500 AI engines**, using real-world fraud signals from more than **1.2 billion calls** to identify and track evolving deepfake tactics across industries. Detection systems aren't just nice-to-have—they're necessary for stopping fraud at the source.

The 2025 forecast: what the data tells us

2024 was a breakout year for deepfake fraud. The insurance industry saw a **+475%** increase in synthetic voice fraud attacks, while the banking industry had a **+149%** increase over the previous year.[1]

This year, however, will be the year it goes mainstream. According to recent projections, in 2025, we can expect:

- **1 in every 151 calls** into the contact center will contain a synthetic voice[1]
- **2% of all fraud** will be driven by deepfakes[1]

2025 PROJECTIONS

Deepfake fraud to rise **+162%**

1 in every 47 calls into the contact center will be a deepfake

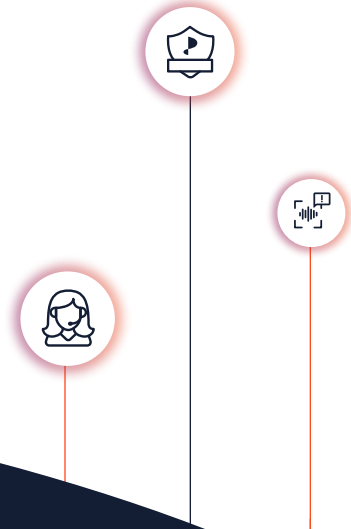
©2025 Pindrop®. All rights reserved.

It's not just happening over the phone. Deepfake fraud is shifting into real-time communications channels commonly used for business, including **Microsoft Teams, Zoom, Slack**, and other web-based support platforms.

Looking forward, we can predict the rise of deepfake-related trends like **synthetic identities**, **AI-generated audio breaches**, and **fully autonomous fraud bots**. These risks are compounded by how accessible and affordable deepfake tools have become.

Businesses need to shift from reactive defenses to proactive detection and continuous monitoring. The longer detection is delayed, the higher the risk of exposure, reputational damage, and financial loss.

[1] Pindrop analysis of non-live calls and fraud data from more than 1.2 billion calls for the year 2024
[2] Stacey James, An Accounting of Financial Professionals, webinar, Medius
[3] Data from Pindrop analysis of 2,490 fraud calls to 10 financial institutions in 2024
[4] Predictions based on Pindrop early fraud data from January–February 2025



Deepfake attacks are here. Are you ready?

The threats outlined in this guide represent only part of the picture. Our Voice Intelligence and Synthetic Risk (VISR) Report has **comprehensive insights from over 1.2 billion calls**, with detailed fraud benchmarks across banking and financial services, insurance, healthcare, retail and ecommerce, and public sector and education industries.

It also includes real-world case studies, attack vector breakdowns, and forward-looking risk models to help your organization plan for the future.

Get the facts and stay prepared

- Want industry-by-industry fraud benchmarks?
- Looking for detection strategies that actually work?
- Curious how Pindrop® Pulse detects deepfakes in real time?

Be the first to read the 2025 Voice Intelligence + Security Report

Packed with data-driven insights to help your business navigate emerging fraud threats.

JOIN THE WAITLIST

©2025 Pindrop®. All rights reserved.