

\ Case Study

How a Global Bank Defends Contact Centers Against Deepfake Threats with Reality Defender



AI Voice Fraud: The Next Cybersecurity Challenge for Call Centers

AI voice fraud has moved from proof-of-concept to real-world impact. High-profile scams involving synthetic voice impersonation have already cost financial institutions tens of millions — bypassing human detection, voice authentication systems, and exploiting operational blind spots in call center environments.

A tier-one global bank, managing billions in daily transactions, observed a rise in deepfaked calls that bypassed standard verification protocols — including voice biometrics and callback checks. While these controls were designed to catch fraud, they weren't built for AI-generated speech. The bank's fraud and risk teams launched a proactive assessment and partnered with Reality Defender to evaluate their exposure to synthetic voice.

The bank's fraud and risk teams partnered with Reality Defender to launch a proactive assessment — an engagement that has since evolved into a production deployment supporting real-time detection across customer-facing teams.



How Reality Defender Exposed AI Voice Threads Missed by Legacy Solutions

The bank’s fraud and innovation teams worked with Reality Defender to analyze recent customer call recordings across Zoom, Meet, NICE, Twilio, and Five9. These calls represented sensitive workflows – like escalations and customer authentication – where synthetic voice could bypass frontline detection.

Reality Defender seamlessly integrated with the bank’s call center and conferencing platforms to detect synthetic voice in real time – without disrupting existing workflows or requiring backend changes.

Our platform returned probability-based risk scores for each file, giving analysts clear, interpretable signals – rather than binary outputs.

Dashboard

VideoGuard

VoiceGuard

Verify Media

Team

Usage

Settings

JD Jane Doe

Voice Calls

Inspect analyzed voice calls from your integrated call systems

Conclusion

Any call direction

Call	Conclusion	Call Source	Receiving
<div> RqDty6WQJRy7qXsw</div> <div>0:1s</div>	... Listening	Genesys	+1 2345
<div> HcVe3t7G4gCauLdU</div> <div>0:1s</div>	... Listening	Genesys	+1 2345
<div> zVaWwFXb451WYBP</div> <div>0:1s</div>	... Listening	Genesys	+1 2345
<div> 4viSV9kMExMNwd8o</div> <div>6/6/2024, 1:31:12 PM</div>	Authentic	Five9	+1 2345
<div> tmiEGnExXYAgb40v</div> <div>6/6/2024, 1:31:12 PM</div>	Manipulated	Genesys	+1 2345
<div> ciSEEQi6fySWkgXr</div> <div>6/6/2024, 1:31:12 PM</div>	Authentic	test-call-5.mp3	-
<div> lySZsAZmbbM2yguv</div> <div>6/6/2024, 1:31:12 PM</div>	Authentic	Genesys	+1 2345
<div> 89GbxVatkaOraXo8</div> <div>6/6/2024, 1:31:12 PM</div>	Manipulated	Five9	+1 2345
<div> RqDty6WQJRy7qXsw</div> <div>6/6/2024, 1:31:12 PM</div>	Inconclusive	Genesys	+1 2345
<div> zVaWwFXb451WYBP</div> <div>6/6/2024, 1:31:12 PM</div>	Authentic	Genesys	+1 2345

Incoming call

tmiEGnExXYAgb40v

6/6/2024, 1:31:12 PM

Conclusion

Time to verdict

Source

Language(s)

Receiving number

Calling number

Manipulated

15.3 seconds

Genesys

English

+1 2345 6789

+1 2345 6789

Call audio

0:03 / 0:15

Segments

0:00 - 0:06

Verdict

Segment ID

Language Detected

Audio Streamer

Audio Everest

Inconclusive

QEGXIE46i27pyuzGhM-qu-UrsZg-RS

English

100% authenticity

96% authenticity

Image 1
Reality Defender's Deepfake SOC Interface



Key Results



Over 1.7M customer calls analyzed in 2024 — across US and LATAM operations



~960 synthetic voice calls detected



Detection delivered in real time to ~600 frontline reps, without disrupting workflows

These findings gave the fraud team new visibility into calls that had gone unflagged by traditional systems — triggering a new internal process for triage and escalation.

Similar deepfake voice scams have cost peer institutions up to \$35M in single incidents — making early detection not just a technical win, but a business-critical one.



How Financial Institutions Can Take Actions Against Voice Fraud

This engagement revealed concrete evidence of synthetic voice risk — and helped define a practical model for detection and response that financial institutions can implement today.

Here's what your teams can do next

- ① Scan for Hidden Risk**
Start with a baseline review of recent recorded calls — focusing on fraud-prone workflows like authentication and executive requests. This test uncovered synthetic audio that had gone undetected.
- ② Build a Triage Layer with Confidence Scoring**
Reality Defender provides risk scores — helping teams triage and escalate based on internal fraud thresholds, not just binary results.
- ③ Deploy Without Disruption**
Reality Defender provides risk scores — helping teams triage and escalate based on internal fraud thresholds, not just binary results.
- ④ Get Ahead of Regulatory Expectations**
AI-driven fraud is drawing scrutiny. Proactive detection is now part of a defensible, modern fraud strategy.

“Our implementation of Reality Defender's AI detection technology exemplifies the bank's approach to security innovation. By integrating Reality Defender into our contact centers, we've added a powerful layer in our defenses against voice fraud. This technology represents an important evolution in how financial institutions can protect high-net-worth clients from increasingly sophisticated impersonation attacks.”

CTO of Private Client Division



Why it Matters Now

- AI-generated voice is being used to impersonate executives, trick agents, and bypass identity checks.
- Frontline teams aren't equipped to detect synthetic speech — and threat actors are exploiting that gap.
- Regulators are beginning to scrutinize how institutions address AI-driven threats — detection readiness may soon be required.

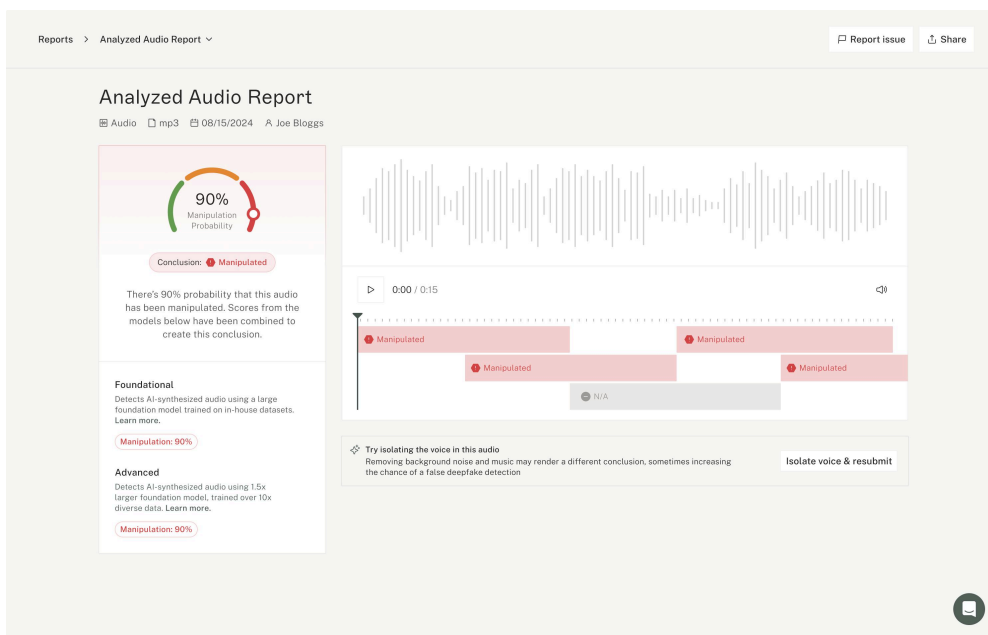


Image 2

Audio report from Reality Defender's Deepfake SOC

Note: This case study has been anonymized. All client identifiers and sensitive data have been removed to preserve confidentiality.



Get in Touch

Reality Defender supports leading financial institutions in building real-time detection capabilities that match the sophistication of today's threats.

Start your risk assessment today at
realitydefender.com