



Ribbon Call Trust – Deepfake Detection

Restore trust in every voice call

Voice communication has always relied on a simple assumption: that we can recognize and trust a familiar voice on the other end of a phone call.

AI-generated voice cloning is changing that assumption. Using a short sample of recorded speech, attackers can create convincing synthetic voices and combine them with caller ID spoofing and social engineering. The result is a call that sounds familiar and credible. Unfortunately, it’s a call designed to deceive and profit from fraud.

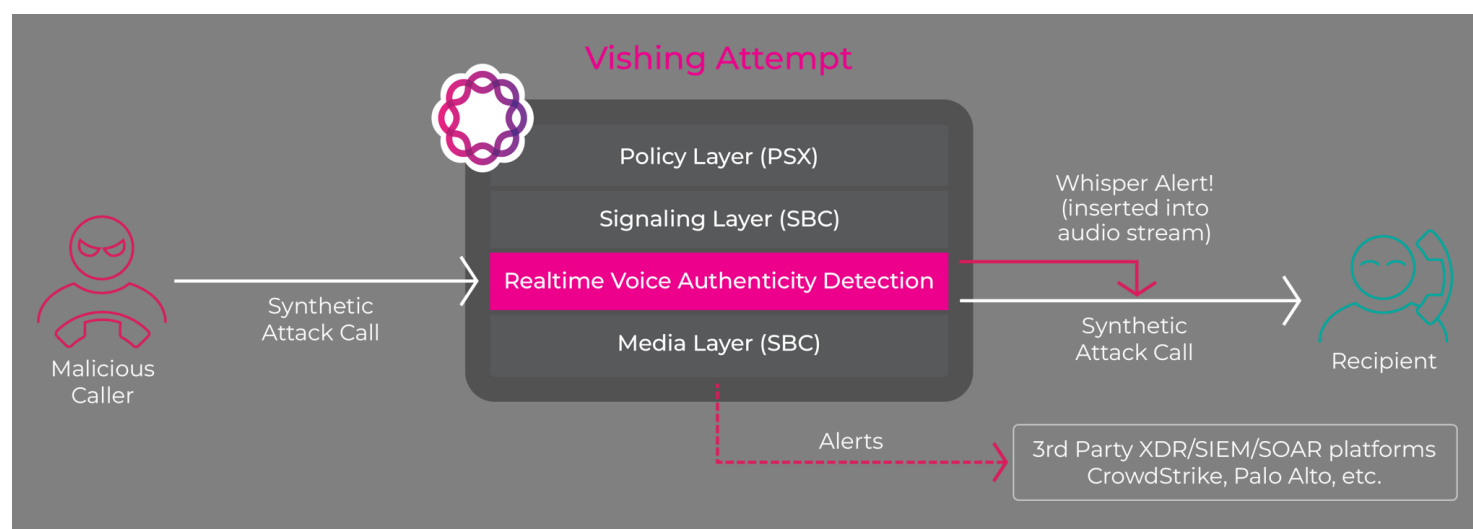
Common deepfake attack scenarios

Executive Impersonation A cloned voice pressures an employee to approve a payment or disclose information.	Customer Service Fraud A caller tries to bypass identity checks and access an account.	IT Help Desk Attack An impersonated employee requests a password reset or a privilege change to access the network.
High-value Personal Information A fake caller targets financial, healthcare, or government information.	Automated Attacks Automation makes voice-phishing campaigns more scalable and applicable to any language.	Hiring Fraud A synthetic identity is used during remote interviews or onboarding.

Ribbon Call Trust – Deepfake Detection helps service providers and large enterprises identify AI-generated calls and warn recipients before trust becomes a liability. Deployed in the core of the voice network, Ribbon’s solution delivers broader threat protection and operates transparently across multiple platforms and use cases..

How it works

1 CALL ANALYSIS An incoming call enters the voice infrastructure and is screened for issues.	2 DETECTION Analytics examine audio and available network signals for indicators of manipulation.	3 RISK EVALUATION The service evaluates whether the voice interaction appears suspicious.	4 USER WARNING The recipient receives an alert before acting on the request.
--	---	---	--



Fraud detection can't be limited to deepfake detection. Ribbon uses a layered strategy that is more effective and uses fewer resources than other solutions.

Call Trust – Deepfake Detection is part of a broader Call Trust portfolio, meaning Ribbon offers multiple tools to stop the next attempt before it happens. Ribbon can look for patterns or see that a specific number or location is generating fraudulent calls. That means that Call Trust can block calls from known bad actors before they saturate the network. The sooner Ribbon intercepts fraudulent calls, the fewer resources required to stop them.

Ribbon Call Trust – Deepfake Detection introduces a network-based layer of protection from deepfake attacks. Instead of relying on a specific smartphone app, UC platform integration, or complex contact-center integration, the service analyzes calls transparently within the communications network and warns users on any device or application. Ribbon protects the telephone line, not a specific endpoint or app.

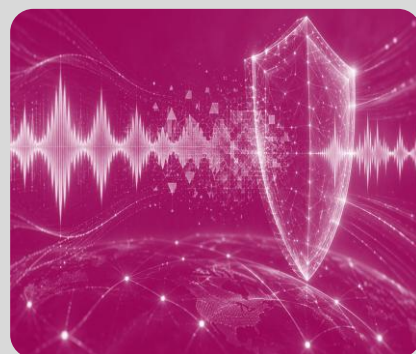
Best of all, since the solution is network-based, IT teams don't have to deploy PC software or cajole users into loading smartphone apps on personal devices. Likewise, there's no worry that a parent or loved one loses protection if they replace a smartphone or still rely on a landline.

Deepfake attacks exploit human trust, not just technical vulnerabilities

Why current defenses leave gaps

- **Limited Access**
Most services only protect a specific device, UC client or contact-center environment.
- **Fragmented Protection**
Different tools don't communicate, giving bad actors immunity from prior attacks.
- **Single Line of Defense**
Relying only on Deepfake Detection ignores the other tools that identify fraudulent numbers and behavior.
- **Human Judgment Under Pressure**
Urgency, authority, and familiarity may overwhelm a victim's concerns about taking a suspicious action.

**Capture → Clone →
Impersonate → Defraud**



Bring Trust Back to Every Call

Ribbon Call Trust – Deepfake Detection identifies potential deepfake threats, warns users, and reinforces confidence in voice communications.

Unfortunately, our community's oldest members are most at risk. While they may not have a financial institution's millions, they also lack the training or safeguards needed to protect themselves.

Even the savviest technologist can be fooled by deepfakes; how would someone who grew up with a rotary phone be prepared for this level kind of deception?

Ribbon Call Trust – Deepfake Detection makes it easy to protect our loved ones and neighbors. The solution stays transparent until you need it. Only then does it alert the user and disconnect the fraudster.

Ribbon's solution supports almost any language. That's important, as AI tools can speak any language like a native. Bad actors will surely expand their reach to new environments where obscure languages previously served as a barrier to access.



When a familiar voice is fake, the network offers the first line of defense.

For Service Providers And Their Subscribers

Differentiate Voice Services Offer protection against emerging AI-driven voice threats.	Create Service Opportunities Package protection within premium or managed security offers.
Build On Voice Infrastructure Extend security at a strategic point in the call path.	Strengthen Customer Trust Show leadership in communications security and fraud prevention.

For Enterprises And Their Customers

Reduce Fraud Exposure Help users recognize suspicious interactions before taking action.	Protect High-risk Roles Add safeguards for executives, finance teams, help desks and contact centers.
Support Layered Security Complement identity, authentication and fraud-prevention controls.	Improve Real-time Awareness Provide real-time warnings when risk matters most.

Copyright © 2026 Ribbon Communications Operating Company, Inc. ("Ribbon"). All Rights Reserved. V1026_1. All other trademarks, service marks, registered trademarks, or registered service marks may be the property of their respective owners.