Whitepaper
Nuance Gatekeeper

Defeating AI deepfakes in the contact center

How to protect your brand and build customer trust in the age of generative AI.

The generative AI market is booming—full of exciting innovations, from advanced chatbots to photorealistic image creation. But every new technology has two sides, and fraudsters are already exploring how they can use generative AI for gain.

The growth of generative AI is fueling new fraud tactics

Fraudsters are experimenting with AI-generated voices as they look for new ways to manipulate organizations and take advantage of their customers. They can use these synthetic voices to hide their identity or assume someone else's while they're on the phone with an institution such as a bank, insurer, or retailer.

Until recently, creating a "clone" of someone's voice required professional audio equipment and hours of high-quality audio—anything less simply wouldn't trick a human ear, let alone bypass biometric security.

But now, advances in AI are allowing almost anyone to create realistic synthetic voices with publicly available tools and just a short amount of spoken or recorded audio. From there, it's as simple as typing out a script for the voice to read.

There are now dozens of different tools for synthesizing voices available on the consumer market—and their low cost and ease of use is making them attractive to fraudsters. Criminals are already using this tech to target individuals, and making the headlines with ransom calls supposedly featuring the voices of kidnapped loved ones.[1]

But synthetic voices are also being used against organizations, and fraudsters are beginning to test out "voice deepfakes" that aim to fool IVR systems or contact center agents into believing they're legitimate customers. And as media attention for this new threat vector grows, more copycats will emerge.

80% of consumers are concerned about AI being used to defraud them[2]

The rise of synthetic voices is compromising trust on both sides of the relationship between consumers and organizations. If a company doesn't have the right protections in place, it can't have full confidence in the voice on the other end of the phone. Many consumers, meanwhile, are worried about whether their bank, internet service provider, or favorite retailer can effectively protect their accounts. Indeed, nearly 80% of consumers say they're concerned about AI being used to defraud them.[3]

If an organization's authentication processes are out of date, their contact center becomes a key vulnerability for criminals to exploit. A successful attack exposes the business not only to extensive fraud losses but significant brand damage that can destroy customer loyalty.

Can my voice really be cloned?

Though it may sound convincing, a synthetic voice is merely a digital imitation—not a true "clone." There are always telltale artifacts in the audio signal that prove it's fake.

Is it easy to clone a voice?

It's simple to create a synthetic voice—but targeting a specific individual is much harder. The fraudster needs access to good-quality audio recordings as well as personally identifiable information (PII) about their victim.

Is biometric authentication still safe?

Modern voice biometrics offer the best line of defense against deepfake attacks, and most other forms of fraud. Legacy authentication methods like security questions and SMS one-time-passcodes are far easier to exploit.

Deepfakes are exerting a new level of pressure on the contact center

Just as it has with more traditional fraud threats, the contact center is rapidly becoming the front line in the battle against AI voice-enabled fraud. For years, fraudsters have manipulated the IVR and agents into giving them access to information and accounts. But success depended on them knowing enough personal details to impersonate the target.

Now, they can also *sound* like their victim, adding another layer of credibility to their scam and widening the pool of potential targets. It's no surprise that from 2022 to the first quarter of 2023, the proportion of "deepfakes" among all fraud types grew by 1,200% in the US alone.[4]

Even when they're not targeting a specific person, synthetic voices allow fraudsters to conceal their identity, create entirely fake personas, and avoid having their real voice recorded.

With a convincing synthetic voice and the right personal information—whether it's for a real person or a fake identity—fraudsters can quickly launch a range of attacks:

— **Account takeover:** Fraudsters use social engineering techniques and a synthetic voice to convince a contact center agent to give out a customer's personal information or account credentials. That information allows them to take control of the account and steal money, make fraudulent purchases, and more. Account takeovers increased by more than 400% in the first quarter of 2023, compared with figures for the whole of 2022.[5]

— **IVR mining:** Fraudsters can use a synthetic voice to phish for new information in the IVR, or to test the validity of information they've already stolen. This allows them to augment their victim profiles with extra details, increase their attack options, and boost their chances of success.

— **New account and subscription fraud:** Combined with a fake or stolen identity, synthetic voices make it easier for criminals to open new fraudulent accounts with credit card companies, take out loans, or use services without paying. Synthetic identity fraud increased 132% across industries between 2019 and 2022, according to TransUnion research.[6]

To achieve these aims at scale and increase their profitability, many criminals are combining synthetic voices with other AI and automation tools. Certain bots, for example, enable multiple simultaneous attacks on a contact center, boosting the chances of success and making fraudulent calls more difficult for analyst teams to keep up with. Text-based generative AI can also help fraudsters create natural-sounding scripts and playbooks for different scenarios, rapidly expanding the range of scams they can attempt.

AI-enabled fraud demands AI-powered defenses

Concerned by these new developments in AI-enabled fraud, some organizations are hesitant to move on from their existing verification methods, such as knowledge-based and two-factor authentication (KBA and 2FA). But the industry has innovated past these methods for good reason: they're simply not secure enough.

KBA and 2FA offer limited protection in exchange for adding high levels of friction to the customer experience. Fraudsters can evade these measures with SIM swaps, caller ID spoofing, and other well-known tactics, while genuine customers sit through lengthy authentication processes and have to remember complex credentials across the dozens of organizations they do business with.

If organizations want to protect their security and maintain the trust they've built with their customers, they can't afford to lose momentum in the fight against fraud.

To outsmart fraudsters using AI, you need better AI. The tools you use for authentication and fraud prevention need to be even more intelligent than the technology that generates synthetic voices, scam scripts, and automated high-volume attacks. You need to be able to accurately verify the person behind every interaction in real time—not just the information they know or the device they have access to. And to do that, you need a multi-layered set of defenses that includes biometrics and AI decision-making.

1,393

US data breaches in the first half of 2023, compromising the personal info of 157M victims[7]

2016

NIST officially denounced SMS 2FA as insecure[8]

Not all voice biometrics solutions are created equal

Limited solutions that only analyze basic voice characteristics may be defeated by a high-fidelity deepfake. The most advanced solutions are continuously optimized to detect synthetic voices from the latest generative AI models and provide multiple layers of defense against deepfakes.

Defeat synthetic speech fraud with Nuance Gatekeeper

For more than a decade, Nuance has been pioneering fraud and deepfake detection capabilities for the contact center, focusing our research and development on building the multi-layered defenses organizations need to protect themselves and their customers.

Our team is constantly testing and enhancing our core biometric algorithms to stay ahead of the latest threat vectors, including generative AI. At the center of that work is Nuance Gatekeeper, a cloud-native biometric security solution that delivers industry-leading authentication accuracy, fraud detection performance, and reliable protection against synthetic speech attacks.

Alongside its biometric capabilities, Gatekeeper provides several layers of intelligent defense against voice deepfake attacks:

— **Intelligent call forensics:** Before a call even connects, Gatekeeper can validate its origins to make sure the call and the phone number are authentic, not spoofed or virtualized.

— **Synthetic speech and playback detection:** The signal from digitally manufactured audio is full of indicators that help Gatekeeper separate fake voices from real ones and identify when a voice is being played from a recording.

— **ConversationPrint:** There's more to an individual's speech than just the sound of their voice. Gatekeeper also analyzes conversation patterns, vocabulary, grammar, sentence structure, and more to bring additional confidence to authentication decisions and identify imposters.

— **Watermark detection:** Many AI voice and text-to-speech (TTS) services automatically embed source identifiers into their audio, which Gatekeeper can quickly spot.

— **Voiceprint locking:** It's rare that a fraudster using a synthetic voice successfully breaks into a target account on the first try. By locking the customer's voiceprint after multiple failed authentications, Gatekeeper ensures even the most persistent fraudsters can't gain access.

Gatekeeper's AI Risk Engine processes all of these signals in real time and generates a single, transparent authentication decision in seconds, whether the engagement takes place in the IVR, with a live agent, or in a digital channel. That means criminals are stopped in their tracks, while real customers enjoy fast, personalized service without feeling interrogated. In addition, Gatekeeper gives fraud analysts full visibility into risk signals and a powerful set of tools to investigate suspicious engagements offline, helping them shut down organized fraud and make sure no attacks slip through the cracks.

Protect your brand. Build trust.

Trust is hard-won in the age of AI—with so many sources of information, new capabilities emerging every day, and fraudsters taking advantage of every advancement.

Your customers need to know they can trust your organization to protect their information and accounts, whether you're managing their investment portfolio or shipping out beachwear for their next vacation. And your business needs to be confident that the person on the other end of the phone is who they claim to be.

Rather than reverting to legacy authentication methods that have proven unreliable and insecure, now is the time to invest in cutting-edge fraud prevention technology that keeps your organization two steps ahead of even the most innovative fraudsters.

LEARN MORE

To learn more about how you can protect your organization and your customers from emerging fraud threats, visit nuance.com/gatekeeper.

Microsoft + NUANCE

Endnotes

[1] (April 29, 2023). Karimi, Faith. "'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping." CNN. https://edition.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html

[2] (2023). Q2 2023 Digital Trust & Safety Index: Fighting fraud in the age of AI and automation. Sift. https://pages.sift.com/rs/526-PCC-974/images/Sift-2023-Q2-Ebook-Index-Report.pdf

[3] (2023). Q2 2023 Digital Trust & Safety Index: Fighting fraud in the age of AI and automation. Sift. https://pages.sift.com/rs/526-PCC-974/images/Sift-2023-Q2-Ebook-Index-Report.pdf

[4] (June 22, 2023). Zholudev, Vyacheslav and Goldman Kalaydin, Pavel. "Deepfakes are the new big threat to business. How can we stop them?" Sumsub. https://sumsub.com/blog/liveness-and-deepfake-detection/

[5] (2023). Q2 2023 Digital Trust & Safety Index: Fighting fraud in the age of AI and automation. Sift. https://pages.sift.com/rs/526-PCC-974/images/Sift-2023-Q2-Ebook-Index-Report.pdf

[6] (2023). 2023 TransUnion Global Omnichannel Fraud Report. TransUnion. https://www.transunion.com/content/dam/workfront-assets/truportfolio/GFS-22-F125939-TruVa-2023OmnichannelFraud-RPR-US_EN-US.pdf

[7] H1 2023 Data Breach Analysis. Identity Theft Resource Center. July 2023. https://www.idtheftcenter.org/wp-content/uploads/2023/07/20230712_H1-2023-Data-Breach-Analysis.pdf

[8] "NIST declares the age of SMS-based 2-factor authentication over." TechCrunch. 25 July, 2016. https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/

About Nuance Communications, Inc.

Nuance Communications is a technology pioneer with market leadership in conversational AI and ambient intelligence. A full-service partner trusted by 77 percent of U.S. hospitals and more than 75 percent of the Fortune 100 companies worldwide, Nuance creates intuitive solutions that amplify people's ability to help others. Nuance is a Microsoft company.

ENT_4895_01_WP, Aug 25, 2023