Microsoft + NUANCE

Brochure
Nuance Gatekeeper

Fight fraud and streamline CX in every channel

How biometric security delivers seamless experiences and protects against fraud across the customer journey.

Contents

As more brands build omnichannel experiences, customers are enjoying seamless, personalized service regardless of how they choose to engage. But customers aren't the only ones who benefit.

The growth of omnichannel engagement should be great news for your brand and your customers. They get more convenient services and support, and you get to drive down your contact center costs with enhanced self-service, not to mention the revenue increase from new cross-sell and upsell opportunities.

But it's not just legitimate customers who are taking advantage of omnichannel.

More channels for your customers also means more opportunities for fraudsters. A wide variety of touchpoints gives them a broader environment to mine for personal information, set up fake accounts and take over genuine ones, make fraudulent purchases or transactions, and socially engineer agents. And if all your channels aren't connected and secured properly, it's easier for fraudsters to cover their tracks by jumping between different touchpoints and hiding their paper trail.

How can you give customers a consistent, friction-free experience across every touchpoint while protecting their accounts and your business from criminals?

More than two-thirds of customers now use multiple channels to complete a single transaction.[1]

Balancing security and customer experience

It's a challenge as old as customer service itself: the more security measures you add to an experience, the less convenient it becomes. Customers know verification processes are there to protect them—but that doesn't make them any less frustrating.

Traditional knowledge-based authentication methods are not only inconvenient; they also aren't as reliable as you might expect. Most of us have forgotten a password, PIN, or the answer to an obscure security question at some point. And it's easy for fraudsters to find this information online or steal it by manipulating agents. Even possession-based security measures such as one-time passcodes (OTPs) can be intercepted through SIM-swap fraud, mobile malware, and social engineering.

Customers want hassle-free access to your services and their accounts, but they also want confidence that their personal and financial information is safe. This requires a new approach to security and authentication.

AI-powered authentication and fraud prevention tools are taking on this dual challenge, helping organizations streamline customer authentication while keeping fraudsters at bay. Achieving this balance is rapidly becoming a key competitive differentiator for brands. But to make a meaningful difference, these solutions need to work across every channel.

89%

of consumers say easy login and authentication processes influence which businesses they decide to interact with online.[2]

The importance of an omnichannel approach to security

According to Forrester, 82% of firms agree that omnichannel authentication is increasingly critical to fraud prevention—but only 59% say their organization is almost or completely optimized.[3]

This isn't sustainable for organizations or their customers. Fraudsters are highly resourceful, and often able to dodge point solutions by attacking a different channel with new tactics. For example, if they're thwarted by transaction analysis online, they might switch to a company's mobile app and try again with a new identity. As new channels join the mix, there are yet more opportunities for fraudsters to evade detection.

These days, fraud is rarely committed by a lone actor hand-selecting accounts to target. Many groups are scaling their activities through automation, using bots to attack multiple channels and accounts simultaneously. In 2022, around 30% of all attacks were classified as automated threats—and it's even worse in retail, where more than 60% of attempts came from "bad bots," according to research by Imperva.[4]

To fight back, fraud teams need a holistic view of threats and the tools to protect customers, track criminals, and prevent fraud regardless of where it happens. Biometric security solutions can help by providing consistently effective customer authentication and fraud prevention that works across voice and digital channels.

> Online and mobile channels are now the leading drivers of fraud costs for financial services organizations.[5]

Fighting fraud in the contact center

The contact center is a high-friction, high-fraud-risk zone. Although customers are embracing self-service, they still want access to a real person when they need it, leading to consistently high call volumes. This became an even greater problem after the pandemic and the resulting shift away from brick-and-mortar. Overburdened agents struggle to service this demand, leading to long hold times.

Most IVRs have limited built-in security, so verification often falls to the agent, and slow, manual authentication leads to longer handle times and frustrated customers. Meanwhile, since these traditional methods are easy to exploit, they minimize friction for fraudsters.

Without automated support, there's a huge amount of pressure on agents to recognize potential fraudsters and "catch them in the act." If the fraudster has all the right information and completes a transaction successfully, it's almost impossible to trace them after they hang up. And it's then easy for them to call again and attack a different agent using someone else's identity.

95.5%

of customers still say they want the option to speak to a human agent when necessary.[6]

How voice biometrics solve the contact center challenge

Voice biometrics can seamlessly verify a caller from their natural speech in seconds as they're talking to the IVR or an agent. This also makes it nearly impossible for fraudsters to access a customer's account. Voice biometrics help contact centers boost security and improve the customer experience in several ways:

— **Containment within self-service channels:** Automated biometric authentication in the IVR helps legitimate customers get help without escalating to an agent, and can prevent fraudsters from ever reaching an agent.

— **Fraudsters can't hide:** On top of personal identifiers like voice and language patterns, AI-driven solutions can analyze phone numbers, network signals, IP addresses, and details about the device the caller is using. By identifying the person behind the interaction, you prevent fraudsters from hiding behind stolen or synthetic identities, no matter what information they've obtained. This information also helps fraud teams track repeat offenders between interactions and across channels.

— **Agents can focus on service, not security:** By automating authentication, you're taking the burden of fraud prevention off your agents' shoulders, letting them focus instead on providing personalized, five-star service for your customers.

Fighting fraud in digital channels

As the popularity of digital engagement channels has grown, security has lagged behind in many organizations, opening the door to fraud. Despite offering a more modern approach to customer engagement, digital channels replicate many security flaws seen in traditional channels:

— **Inconvenient security measures:** Most online accounts still rely on passwords and security questions to access services—difficult for customers to remember and easy for fraudsters to steal, crack, or buy. With customers reusing passwords between different brands and services, one security breach can put multiple accounts at risk.

— **One-time passcodes:** OTPs are currently one of the most popular methods for adding an extra layer of security, but they don't do enough to protect accounts. Possession of an OTP only proves an individual has access to the right account or device, which can be intercepted or faked through SIM-swapping, malware, or social engineering.

— **New and expanding fraud risks:** Bot attacks are becoming more sophisticated and increasingly difficult to detect using legacy defenses, putting businesses and their customers at higher risk of automated phishing, brute force attempts, credential stuffing, CAPTCHA bypass, and other threats.

52.2%

global growth in suspected digital fraud between 2019 and 2021.[7]

Multimodal biometrics cover modern digital channels
Thanks to the high fidelity of modern voice biometrics, the same data captured through the contact center can be used in digital channels to protect high-risk transactions, logins, account recoveries, and other engagements. In fact, once a customer has enrolled, they can use their voice for seamless and secure access in any other channel, using any device with a microphone. The universality of voice saves customers considerable time and frustration normally associated with account security, and it gives businesses the ability to intercept and track fraudsters using their voice, wherever they choose to attack.

Conversational biometrics, another emerging form of security AI, help secure digital experiences by analyzing factors unique to the individual in messaging interactions such as live chat, virtual assistants, and email. Conversational biometrics build an accurate assessment of the person contacting your organization by analyzing their vocabulary, sentence structure, spelling, punctuation, and emoji usage. If their conversational pattern matches that of the legitimate customer, you can authenticate in real time and provide fast, personalized service. If the pattern doesn't match, or if it matches that of a known fraudster, you can prevent the attack before it happens and gain greater intelligence for ongoing fraud investigations.

These measures stop fraud at the beginning of an engagement, without requiring complicated step-up protocols or multi-factor authentication. Real customers are verified in seconds without any extra effort—and fraudsters are cut off, even if they've managed to acquire personal information. Crucially, once a fraudster or fraud ring has been identified using biometric data, their watchlisted status follows them between channels, so they can't simply regroup and try again somewhere else.

Streamline and protect the entire customer journey

Effective fraud prevention is inextricably tied to customer experience. To keep your customers happy, you have to prioritize the security of their accounts and assets—fraud victims are much more likely to switch to a competitor. But the way you protect customers from fraud has a significant impact on their experience, and you still must meet their expectations for effortless engagements.

Traditional security methods and point solutions fall short in this environment, making customers jump through hoops to be verified, and leaving an incomplete picture of threats across channels. The secret ingredient to seamless and secure omnichannel engagement is found in AI-powered solutions that identify the person behind the interaction, regardless of channel or device. This technology makes it possible to embrace self-service and provide customers seamless experiences without stretching fraud teams to their limit.

As you're evaluating solutions, it's critical to involve decision-makers from across the business, including fraud, security, CX, and contact center leaders—all of whom have a vested interest in fraud prevention and authentication. AI-driven biometric security will allow them to work together in new ways to not only meet customer and business needs, but to strengthen your organization's competitive advantage in the face of an ever-evolving fraud challenge.

Secure experiences effectively in an omnichannel environment
The security measures you choose should meet several key requirements:

— **Enhance, not detract** from the customer experience.

— **Secure interactions across every channel**—not just the contact center.

— **Intelligently identify and track fraudsters** wherever they try to attack your organization or customers.

— **Provide a centralized view** of threats to help analysts assess risk and proactively mitigate fraud.

— **Remove the authentication burden** from agents and customers, wherever they engage.

Fight fraud in every channel with Nuance Gatekeeper
Security solutions founded on AI and biometrics provide more effective tools for fraud detection and investigation, helping you protect customers and your business with less time and effort. To deliver reliable security and seamless CX in an expanding omnichannel world, you need a solution that can handle the most modern threats at scale.

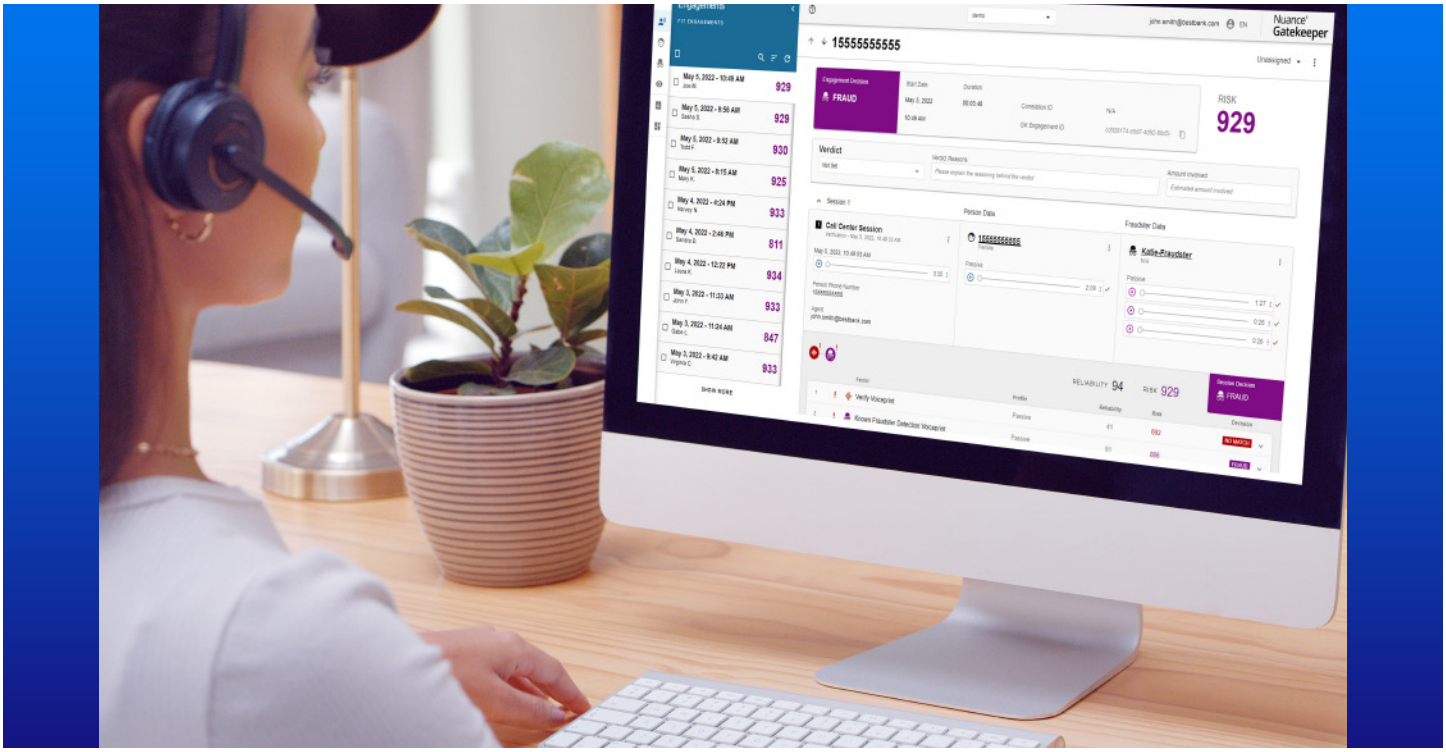
Nuance Gatekeeper is the only solution that provides seamless biometric authentication and intelligent fraud detection across contact center, IVR, web, mobile, and messaging channels.

Gatekeeper uses deep neural networks to analyze millions of factors about a person's voice and how they communicate as they interact across touchpoints, automatically authenticating them in seconds—or identifying them as a fraudster. Our customers have seen 99% authentication success rates, more than 90% accuracy in detecting known or suspected fraudsters, and 92% reductions in fraud losses.

No more interrogating customers for their mother's maiden name. No more burdening agents with lengthy authentication processes when they should be focusing on experience. And no more letting fraudsters slip through the cracks because your fraud analysts are overstretched. With Nuance Gatekeeper, you can build engaging experiences your customers will love, while protecting their information—and your business—at every turn.

AI and machine learning in anti-fraud programs will double over the next two years.[8]

LEARN MORE
Stay one step ahead of fraudsters with Nuance Gatekeeper. Learn more at nuance.com/gatekeeper, or email cxexperts@nuance.com.



Microsoft + NUANCE

Why Nuance?

20+	500+	$4B+	600M	8B+
years of industry expertise	Worldwide deployments	Annual fraud savings	Biometric prints	Annual transactions

Endnotes

1 Stepaniuk, David. (April 19, 2022). Unified Commerce: The New Buzzword Needed Because We Messed Up Omnichannel. Netguru. Retrieved December 12, 2022 from: https://www.netguru.com/blog/unified-commerce-omnichannel
2 Global Digital Fraud Trends: Rising Customer Expectations Amid Evolving Fraud Threats (April 2022). TransUnion.
3 Navigating the Omnichannel Fraud and Authentication Landscape: How Biometrics Power Modern Authentication and Fraud Prevention Strategies (June 2019). Forrester.
4 The State of Security within eCommerce (2022). Imperva.
5 10 Trends That Will Shape the Fraud Landscape in 2022 (2022). LexisNexis.
6 2021 Global Customer Experience Benchmarking Report (2021). NTT.
7 2022 Global Digital Fraud Trends Report (2022). TransUnion.
8 2022 Anti-Fraud Technology Benchmarking Report (Feb 2022). Association of Certified Fraud Examiners.

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_4819_01_B, Jan 25, 2023