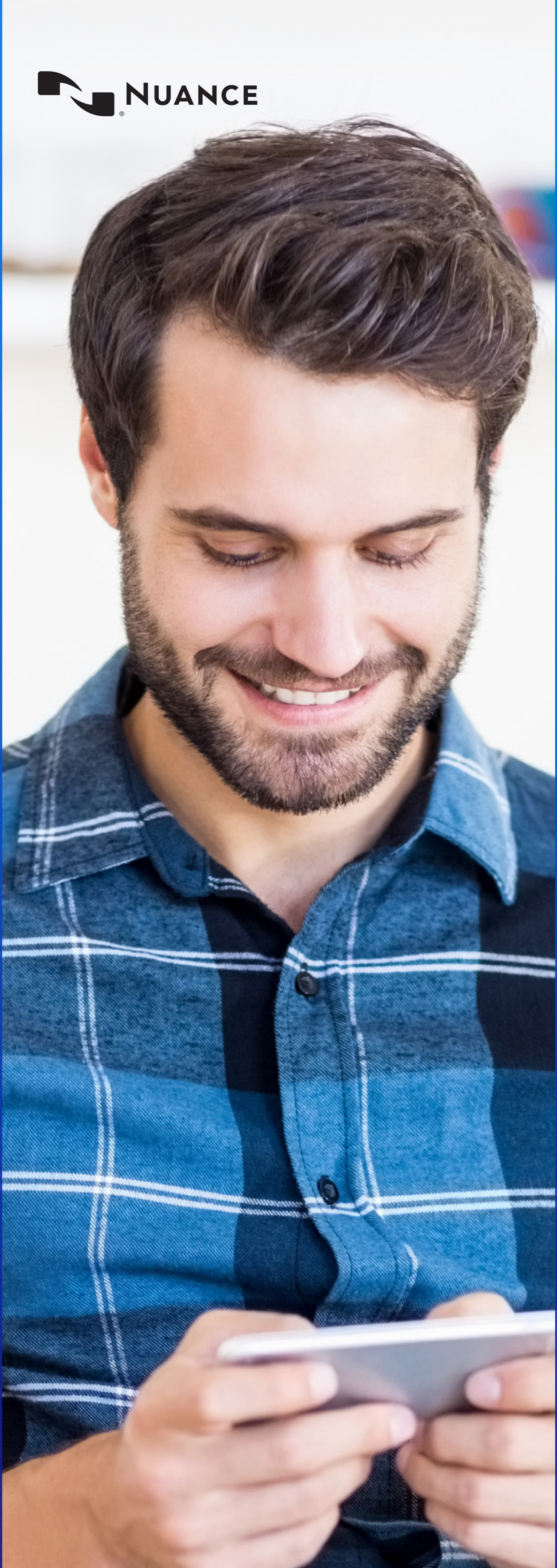


Guide
Nuance Gatekeeper

Preventing fraud in digital messaging

How conversational biometrics help fight the rising tide of fraud.

Contents

Digital engagement is booming. And so is fraud.

Since the start of the pandemic, we've seen a massive shift toward digital customer interactions. More organizations are doing business and serving customers through online channels such as mobile apps and live chat.

Customers now expect to have the simplicity and convenience of engaging with organizations through digital messaging, so they can get support without having to wait in long call queues. But just as in any period of significant change, fraudsters have been quick to take advantage. As organizations and their customers have embraced digital messaging, fraudsters have seized the new opportunity for conducting scalable operations in a poorly protected channel.

Many organizations are unprepared to deal with the simultaneous growth of chat interactions and the surge in online fraud and abuse—but there are ways to protect customers and take the fight to the fraudsters.

In this guide, we'll explore how you can use Nuance Gatekeeper's conversational biometric capabilities in digital messaging channels to intercept fraudsters in real time, and to power deep fraud analysis that results in even greater loss prevention.

22%

global growth in digital customer interactions during the pandemic[1]

1 in 3

consumers globally now conduct more than half of their transactions online[2]

52.2%

global growth in suspected digital fraud between 2019 and 2021[3]

Why digital is an easy target

Fraudsters are opportunists and tend to follow the path of least resistance, and digital messaging channels offer a particularly attractive target.

As organizations took steps during the pandemic to secure their voice channels against increasing fraud, rolling out enhanced security measures like voice biometrics, many fraudsters shifted their efforts to digital channels. In the digital world, a little information can take fraudsters a long way, helping them access accounts, abuse policies, and commit other crimes.

And that information is readily available if you know where to look. Fraudsters are constantly scraping social media and buying and selling stolen customer data on the dark web.

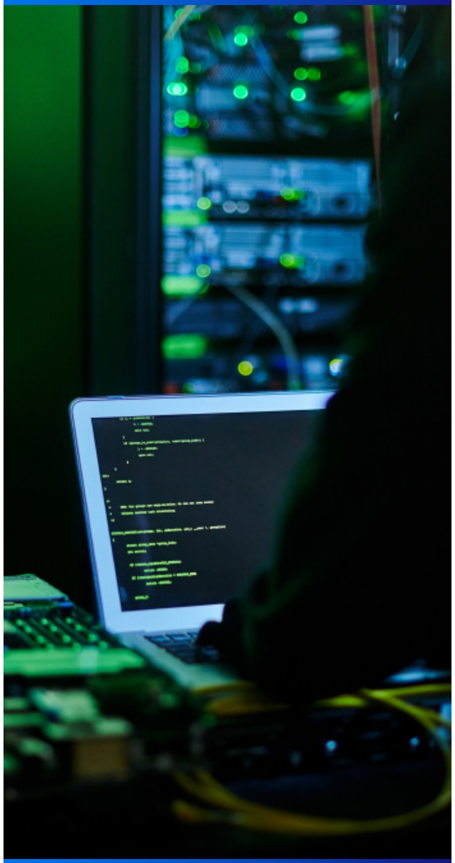
Exploiting vulnerabilities in live chat

Live chat has become a prime target for fraudsters because it allows them to bypass the heightened security protocols of the contact center and socially engineer agents. They can gain access to funds or account details, conduct fraudulent transactions, and request refunds and promotions—all without raising suspicion.

Committing fraud in live chat is also much more scalable than attacking a contact center. Fraudsters can run multiple chat sessions from different devices simultaneously, or even use inexpensive, easily programmable bots to attack many targets at the same time.

Live chat isn't just vulnerable to professional criminals; it's also easier for legitimate customers and amateur fraudsters to abuse policies and business processes for personal gain. For example, a non-professional might abuse a new customer promotion by opening multiple new accounts using fake credentials.

Digital messaging channels are growing in popularity, but aside from basic knowledge-based authentication (KBA), they're largely underprepared for the scale of the growing fraud problem.



24 billion

account username-password combinations are for sale online, including bank accounts[4]

Prevent and detect fraud with conversational biometrics

Current authentication and fraud prevention methods in digital messaging are still mostly information-based. They verify customer identities based on something the person knows, like an order number, email address, username, or password. But as we've seen, this information is easy for fraudsters to obtain.

Many organizations try to enhance security by using step-up verification, such as sending an SMS one-time-passcode (OTP). But again, it's simple for fraudsters to bypass this kind of two-factor authentication. OTPs only verify that someone has access to the phone number or device; fraudsters have various tactics for taking control of a victim's device, diverting OTPs to a device they control, or socially engineering their victims to give them the OTP.

Our biometric security solution, Nuance Gatekeeper, identifies the actual person behind the engagement based on unique characteristics inherent to who they are, no matter what device or identity they hide behind. In the voice channel, Gatekeeper does this by comparing hundreds of voice characteristics in audio signals from callers to saved voiceprints of customers and known fraudsters.

In digital messaging channels, a fraudster isn't speaking, but they're still communicating, and there are still hundreds of factors that make each person unique. That's where conversational biometrics come into play. In Gatekeeper, we call this capability ConversationPrint.

ConversationPrint uses AI to analyze how a person uses language—including their word choice, grammar, sentence structure, emoji usage, and many other elements—and then translates this into a mathematical model.

Gatekeeper uses this model to prevent fraud attempts during interactions by comparing the conversational pattern of the person typing to the pattern of the real customer, and to conversation patterns associated with known fraudsters. ConversationPrint helps you stop fraud in digital messaging before it happens, while powerful analytics uncover more fraud after the interaction.

Uncovering more digital messaging fraud

Nuance evaluated thousands of chat conversations from a major US retailer using Gatekeeper's ConversationPrint and found:

4

repeat offenders for every 1 flagged message

3x

more suspicious sessions overall than originally reported

$10M

in preventable fraud losses

Prevent fraud in real time

When someone contacts one of your agents through digital messaging, you can verify basic credentials through a login or KBA process while ConversationPrint works seamlessly in the background to provide biometric fraud prevention throughout the engagement.

When a fraudster repeatedly initiates chat sessions with your agents using similar narratives or language, or even when they recruit a group of people to run the same fraud scheme, ConversationPrint can detect these patterns and alert your agents in real time.

From there, you can pivot into step-up authentication or ask the person to call in to complete their request over the phone, where you can use voice biometrics to further secure the interaction.

And because ConversationPrint runs invisibly in the background, your legitimate customers get seamless, secure service without the inconvenience and frustration of multifactor step-ups and time-consuming escalations.

Detect fraud asynchronously

After a chat session ends, ConversationPrint provides fraud teams with powerful analytics and detection tools to help them uncover more fraudsters, fraudulent engagements, and fraud narratives.

— **Watchlisting:** Add known fraudsters attacking your digital messaging channel to a watchlist, so you can instantly detect new fraud events they commit in the future.

— **Clustering:** Identify previously unknown fraudsters based on correlation factors such as chat frequency, scripting, and conversation patterns. This helps you find repeated fraud attempts from multiple unknown fraudsters simultaneously.

— **Backward search:** Compare a single conversational pattern with patterns from historical interactions to see if a newly identified fraudster has tried or succeeded at accessing your system in the past.

Adapt business processes to beat fraud

Use what you learn about fraudsters to adapt the customer experience to favor desirable engagements and deter undesirable engagements. For example, after a customer has been flagged as an abuser, you can limit their access to promotions and premium services that pose a greater risk to the business, helping deter non-professional fraudsters.

Seamless, secure omnichannel customer journeys

Nuance Gatekeeper is the only solution that offers true omnichannel fraud prevention and detection capabilities to provide a consistent customer experience and mitigate fraud wherever it occurs. Gatekeeper layers voice, conversational, and behavioral biometrics with non-biometric environmental factors into a central AI Risk Engine that generates a single risk score for every interaction.

This removes the fraud burden from your agents, who no longer have to interrogate customers and make judgment calls about their authenticity. It makes life simpler for customers, who get the service they need through lightning-fast, effortless authentication. And it makes it easier for your organization to offer personalized, predictive experiences while stopping fraudsters in their tracks.

LEARN MORE

To explore your own Gatekeeper solution today, visit nuance.com/Gatekeeper, or email cxexperts@nuance.com.

Endnotes

[1] LexisNexis. (2022). 10 Trends That Will Shape the Fraud and Identity Landscape in 2022. LexisNexis. https://risk.lexisnexis.com/insights-resources/infographic/fraud-and-identity-trends

[2] TransUnion. (2022). 2022 Global Digital Fraud Trends Report. TransUnion.

[3] TransUnion. (2022). 2022 Global Digital Fraud Trends Report. TransUnion.

[4] Digital Shadows Research Team. (2022). Account Takeover in 2022. Digital Shadows.

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_4767_01_B, Oct 19, 2022