NUANCE | WHAT'S NEXT BLOG

Customer engagement, Contact Center AI

Rethinking the agent experience, part 3: Remove the customer authentication burden

Tony Lorentzen | General Manager & Senior Vice President, Intelligent Engagement

June 7, 2023

The third article in our series exploring how to improve the agent experience looks at how traditional authentication methods affect agents, customers, and the business—and how AI can remove the burden of authentication entirely.

In the previous articles in this series, we explored how to improve agent efficiency and increase agent satisfaction. This installment pulls together those themes by looking at how removing the burden of customer authentication can transform agent and customer experiences—while strengthening security and reducing fraud losses.

The authentication burden: bad for agents, customers, and the business

A recent global survey of contact center agents and leaders by CCW Digital, sponsored by Nuance, revealed that 30% of agents find authenticating customers difficult or frustrating. As so many contact centers still rely on passwords, PINs, and security questions for authentication, it's no surprise that agents are frustrated.

Interrogating customers for security credentials can be a lengthy process. And customers often forget or lose their details, adding further time and frustration before they can get to the reason for their contact. Fraudsters, on the other hand, can buy or steal all the information they need to pose as legitimate customers.

The survey showed that three-quarters of contact center leaders rely on agents to handle some or all of the authentication process, and only 12% of agents say they have no responsibility for authentication.

That means agents, who are rarely hired as fraud prevention specialists, play a critical role in protecting customers and the business from fraud. The trouble is, they depend on outdated and unsecure authentication methods.

Traditional knowledge-based authentication (KBA) processes have a negative business impact in several ways:

- **Agent frustration:** Authenticating customers is dull and repetitive, and often agents have to make on-the-spot decisions about the fraud risk of each interaction.
- **Customer friction:** Authentication adds time and effort for customers, even if their inquiry is easy to resolve.
- **Poor personalization:** Customers expect brands to know them, but each interaction starts with customers having to prove who they are.
- **Weak security:** Fraudsters can readily acquire stolen KBA details, making it easy for them to bypass traditional authentication checks.

Remove the burden with biometric security

By deploying advanced biometrics solutions, organizations can leave behind the problems of inefficient, inconvenient, and unsecure authentication methods.

Nuance Gatekeeper provides cloud-native biometric security in every channel to create simple, friction-free experiences for agents and customers—and make life much harder for fraudsters. Gatekeeper authenticates customers based on biometric factors inherent to who they are rather than relying on something they know or a device they control.

For example, Gatekeeper uses voice biometrics to verify caller identities by measuring the sound of their voice against millions of invisible parameters and comparing the result to the "voiceprint" of the real customer. The solution can also detect recorded and synthetic voices—even those created by today's sophisticated generative AI models.

With the addition Gatekeeper's conversational biometrics, the solution becomes even more powerful across channels. ConversationPrint analyzes how people use language during text-based interactions—including word choice, grammar, sentence structure, spelling, emoji usage, and other factors— and compares this to the conversational pattern of the claimed customer.

Alongside biometric factors, Gatekeeper's intelligent call forensics can inspect each call and device before it reaches the IVR or a live agent, checking for signs of fraud such as hidden network origins, virtualized numbers, and spoofing.

A central AI risk engine brings all these factors together to create a risk score for each interaction in seconds, giving agents confidence that they're serving a legitimate customer, and alerting them to potential fraud before it happens.

Biometric security from Gatekeeper transforms the impact of customer authentication:

- **Reduced pressure on agents:** Freed from the burden of manual authentication, agents can focus on serving and selling.
- **Frictionless customer experience:** With no more lengthy interrogation processes and no need to remember security details, customers get faster helpwith less effort.
- **Effortless personalization:** Agents know exactly who they're interacting with from the start of the engagement, so they can easily personalize the customer experience.
- **Strong security:** Biometric security prevents most fraud before it happens, reducing fraud losses and detecting new threats across channels.

Next time: Agent Coach deep-dive

In the final article in this series on the new world of agent work, we'll take a look under the hood of Agent Coach, our AI-powered solution that proactively gives agents real-time information, advice, and recommendations.

Tags: Contact center strategy, Nuance Gatekeeper, Authentication & fraud prevention, Agent experience, Agent Coach

About Tony Lorentzen

Tony has more than 25 years of experience in the technology sector, spending the last 17 with Nuance where he is currently the SVP of Intelligent Engagement Solutions within the Enterprise Division. Before that he served as the leader of several teams at Nuance including Sales Engineering, Business Consulting, and Product Management. A proven leader in working with the cross-functional teams, Tony blends his in-depth knowledge of business management, technology and vertical domain expertise to bring Nuance's solutions to the Enterprise market, partnering with customers to ensure implementations drive true ROI. Prior to Nuance, Tony spent time at Lucent and Verizon where he led teams that applied the latest technologies to solve complex business issues for large enterprises. Tony received a B.S. from Villanova University and a MBA from Dowling College.

View all posts by Tony Lorentzen