What's next

Enterprise

How telcos can power up personalization with biometrics

Under pressure to meet growing customer expectations, personalization is at the top of many telcos wish lists. But personalized experiences can't come at the expense of security and with fraud attacks growing more rampant, carriers can struggle to strike the right balance. Simon Marchand, Nuance's Chief Fraud Prevention Officer, looks at how telcos can offer more personalized experiences without compromising customer security.

Simon Marchand, CFE, C.Adm.

Posted February 23, 2022

It's been a challenging couple of years for telcos as they've tried to keep pace with a rapid shift in customer habits and expectations. We are looking forward to attending Mobile World Congress again this year to talk with CX and fraud leaders about how they're planning to meet new expectations while keeping customers protected.

One theme that's sure to be a major talking point at MWC is the move toward greater personalization of experiences to improve customer satisfaction and increase revenue. AI in various forms will be vital for harnessing customer data to enable personalization. But to deliver truly personalized experiences throughout the customer journey, everything starts with one particular branch of AI: biometric authentication. After all, you can only personalize the experience if you know who you're talking to.

Know who your customers are

When customers are expecting the personal touch, they don't want to face a lengthy authentication process that insists they prove their identity before they can get on with their inquiry.

Biometric authentication offers the fastest, most secure way to know exactly who's at the other end of an interaction. Passive voice biometrics solutions, for example, can authenticate customers in the background of a call by comparing the first few seconds of natural speech with their "voiceprint" as they talk to a conversational IVR, using natural language. That eliminates the effort and frustration of remembering PINs, passwords, and answers to security questions.

By adding a biometric security layer on top of other authentication factors like call validation, the IVR can greet customers by name and begin helping them with their inquiry right away. The most advanced systems can even pull in data from recent interactions with the brand to predict a customer's needs and create upsell and cross-sell opportunities.

And when customers want or need to talk to a live agent, biometric authentication helps agents deliver a personalized experience. Agents no longer need to interrogate callers for security information and then make a judgment call on whether they are who they say they are. Instead, they can focus on understanding what the customer is trying to achieve, helping them reach a fast resolution.

This partnership between agents and AI is something we feel strongly about at Nuance. One of the largest mobile carriers in the US is a long-standing customer, and by connecting customer engagement across automated and live agent interactions, it's seen dramatic increases in CSAT and conversion rates.

Keep your customers protected

Personalizing and streamlining customer interactions offers immense value for customers, agents, and the business. But it's all for nothing if those interactions aren't secure.

Telcos have seen an alarming increase in SIM swap fraud, account takeover attempts, and

other fraud attacks in recent years, and in the rush to offer personalization, it's essential we also stay focused on account protection.

Fraudsters can easily buy, steal, or intercept everything they need to get around traditional knowledge-based authentication processes. They can also use social engineering techniques (or straight-up bribery) to get customer information from agents.

But fraudsters can't steal or spoof a customer's voice (advanced biometrics solutions can detect recordings and synthetic voices), so there's no way for them to fool the system and gain control of a customer's account. And because biometric authentication means agents don't need to see sensitive information to validate a customer's identity, they can't give that information to fraudsters.

So, by adding a biometrics layer to their security, brands can offer streamlined, personalized engagements with confidence that their customers—and their brand—are protected.

Biometrics-enabled personalization in action

Many large telcos are already using biometric authentication to help protect customers and offer them seamless, personalized experiences.

When Deutsche Telekom implemented voice biometrics as part of Nuance Gatekeeper, it wanted to keep customers safe, but its primary goal was to offer them a simple, friction-free experience. With Gatekeeper, Deutsche Telekom customers create a voiceprint and then get instant access to their account the next time they call in. It's a far cry from the world of remembering lengthy ID numbers, and of the 700,000 customers who've registered their voiceprint so far, 75% say it's more convenient.

One of my favorite examples of the power of biometrics the personal touch was implemented by Telefónica. In the early months of the COVID-19 pandemic, the company wanted to ensure vulnerable customers could access support during a massive spike in contact volumes. It used Nuance voice biometrics to identify anyone calling in who was over the age of 65 and then route them directly to priority service.

Where next for telco personalization?

I'm sure that MWC will showcase many more examples of customer experience personalization from telcos all over the world. There's certainly an exciting opportunity right now for carriers to use biometrics to enable greater (and more secure) personalization that increases customer satisfaction, trust, and loyalty.

Tags: Biometric Authentication, Gatekeeper, intelligent fraud prevention, personalization, Telco

More Information

Two-factor authentication is broken. Let's fix it.
Download the whitepaper
Learn more

About Simon Marchand, CFE, C.Adm.

Simon Marchand is Nuance's chief fraud prevention officer for security and biometrics. Certified Fraud Examiner, Simon has extensive expertise in fraud prevention, detection and management - as well as in authentication and identity - in both the banking and telecom industries, with more than 10 years of experience in the field. Prior to Nuance, Simon held key fraud prevention positions at Montreal-based Laurentian Bank, at Bell Canada, and at Québec's Order of Chartered Administrators, where he managed its professional inspection program. As chief fraud prevention officer, he works closely with Nuance clients to design biometric-based fraud prevention and authentication strategies that disrupt criminals while reducing effort and friction for legitimate customers. He regularly shares his expertise in various conferences and with associations around the world and he speaks on the risks of fraud and the ethical use of biometrics in the media.

View all posts by Simon Marchand, CFE, C.Adm.