What’s next

Enterprise

Security customers can’t see, and fraudsters can’t beat

Security—and how to make it invisible to customers—is just one of the key themes we’ll be discussing with global customer engagement leaders at this year’s Nuance Customer eXperience Summit in London on March 10.

Brent Hunt
Posted 31 January 2020

Put aside (if you can) the pressures of delivering amazing customer service experiences while reducing your cost to serve. The bottom line for customer engagement is that outstanding, cost-optimised experiences can’t come at the expense of security.

That’s why security—and how to make it invisible to customers—is just one of the key themes we’ll be discussing with global customer engagement leaders at this year’s Nuance Customer eXperience Summit in London on March 10.

It promises to be great event, and a fascinating discussion, but to kick things off, let's take a look at why security is such a hot topic in customer engagement right now. And while we're at it, we'll also look at some of the tech breakthroughs that can revolutionise your approach to customer authentication and fraud prevention.

The cross-channel security challenge

As brands got smarter about adding more engagement channels to increase convenience for their customers, fraudsters got smarter about hopping between those channels to commit their crimes. Often, fraudsters will socially engineer contact centre agents before using the information they've gathered to perpetrate fraud on other, less protected channels.

Here's Forrester on the cross-channel conundrum (you can get the analyst's full research findings here):

- "82% of firms agree that authentication across channels is increasingly critical to fraud prevention. Yet only 59% define their cross-channel fraud prevention as nearly or fully optimized."

As Forrester highlights, the biggest challenge for cross-channel fraud prevention is organisations' use of traditional knowledge-based authentication (KBA) methods. PINs, passwords, and PII are all available cheaply on the dark web, rendering them useless for customer authentication. They're also easily forgotten by genuine customers, adding friction to customer engagements and increasing the number of false positives that fraud prevention teams have to deal with.

Does biometrics tech hold the answer?

Many organisations are turning to biometrics technology to support their cross-channel security strategy. Using multiple biometrics modalities in the contact centre and across digital channels can be an effective way to quickly and accurately authenticate customers and minimise fraud risk. Less effort, less fraud: that's the biometrics win-win.

Voice biometrics, for example, authenticates customers and identifies fraudsters by rapidly analysing hundreds of variables in people's voices. In fact, our own Nuance Lightning Engine is powered by algorithms that can authenticate callers in the IVR or contact centre with less than two seconds of audio and with 25%-40% better accuracy than previous generation technology.

In digital channels, **behavioural biometrics** analyses patterns in how individuals interact with websites and apps on their keyboard, mouse, or smartphone (alongside many other behavioural characteristics) to complete a task—patterns that are incredibly difficult for

fraudsters to replicate.

And the biometrics innovations keep on coming. In fact, one of my colleagues here at Nuance has invented an entirely new modality of biometrics. The **'conversational biometrics'** tech in our ConversationPrint solution takes voice biometrics one step further, analysing people's vocabulary, grammar, sentence structure, and more to create a unique profile of how they use language during interactions.

If you'd like to find out more, you can read all about how ConversationPrint made it from brilliant idea to exciting new product. We've got the inside story from its inventor in the latest, security-themed edition of our digital magazine, Nuance IQ.

The future of secure, effortless authentication at CXS20

There's huge potential for organisations to use a combination of these biometrics technologies to enhance security across all channels while reducing customer effort to the point where security becomes invisible.

Join us at the Customer eXperience Summit to discover the future of invisible security—and learn what's next for personalized, predictive, channel-less customer engagement.

Tags: Authentication Biometrics, Forrester

More Information

Apply now and join us in London
Apply to attend this year's event
Learn more