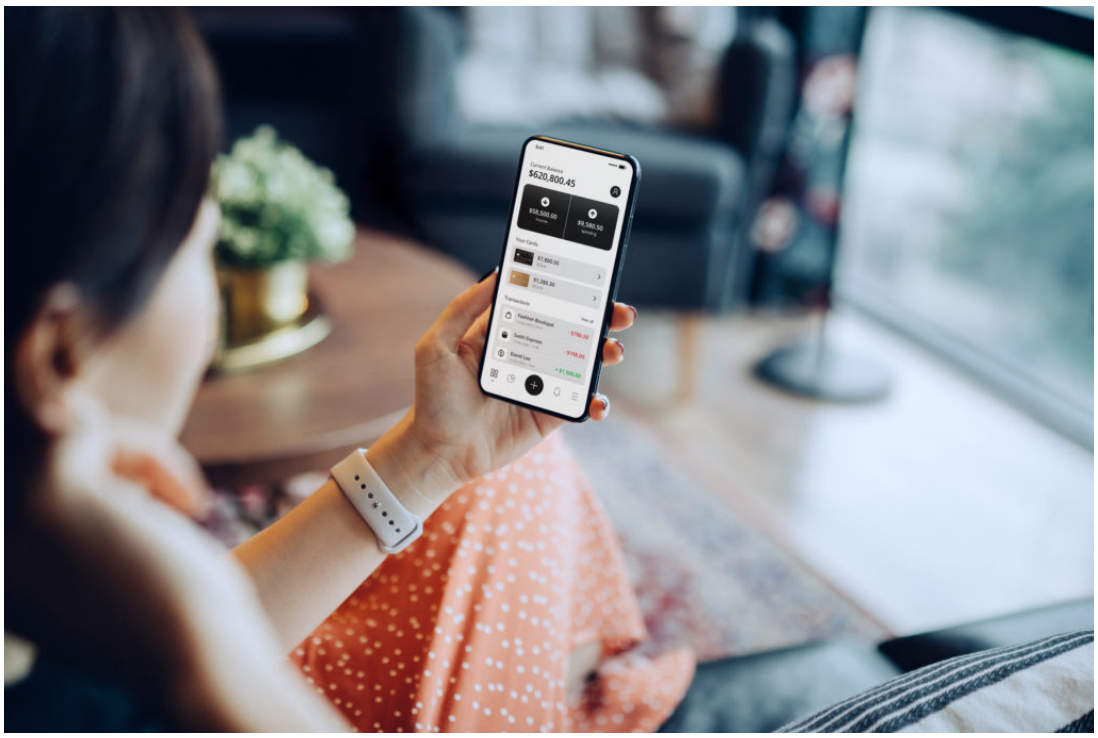
NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

It's time to rethink customer authentication

Brett Beranek | Vice President & General Manager, Security & Biometrics

26 October 2021



It's Cybersecurity Awareness Month and, once more, the world is reminded that the knowledge-based authentication methods we trust to protect us aren't up to the task. But it's not time to call the win for the fraudsters just yet. With biometric authentication, enterprises are protecting consumers like you and I—and providing superior customer experiences at the same time.

It makes sense that Halloween comes at the end of Cybersecurity Awareness Month, because the numbers are terrifying.

Consumers worldwide lose billions every year to fraud and, earlier this year, a global survey by Nuance found that one-fifth of respondents had been the victim of fraud in the previous 12 months. The problem is getting worse; a security leader at a retail bank that I spoke to recently told me they'd seen a 400% rise in fraud attempts during the COVID-19 pandemic.

Far too many people and businesses still rely on authentication tools that are no longer fit for purpose. And the disruption of the last 19 months has created new opportunities for fraudsters to exploit. That's why it's more urgent than ever to move away from traditional customer authentication methods like PINs and passwords to stronger factors like biometrics.

There's no such thing as a strong password

It's very easy for criminals to buy PINs, passwords, and other personally identifiable information (PII) on the dark web. And poor password hygiene compounds the problem, making those stolen credentials even more valuable for fraudsters.

Our survey revealed that—despite all the publicity and education around cybersecurity awareness—76% of consumers still don't use different passwords for every website or brand they interact with, and only 18% follow "password strength" indicators and choose the strongest option.

So, if traditional authentication methods can't provide adequate security, it must at least offer a good customer experience, right?

Wrong. Knowledge-based authentication (KBA) methods create almost no friction for determined fraudsters, who always have all the information they need. But these methods add significant friction for genuine customers, who often lose or forget the information that's supposed to verify their identity. Do *you* remember your first-grade teacher's last name, or your 16-digit customer number?

Survey respondents say traditional authentication methods are damaging the customer experience. Almost a third (31%) get frustrated with upper and lower cases and special characters, and 30% have regular issues with remembering usernames, PINs, or passwords and having to reset them.

The time has come for biometric authentication

To address the inherent vulnerabilities of traditional KBA methods, many enterprises are turning to biometric authentication. Solutions like Nuance Gatekeeper verify people's identities based on characteristics that are unique to each of us as an individual. These factors can't be forgotten, stolen, or spoofed—making them both more secure and more convenient.

While device-based biometrics like fingerprint and facial ID systems are well-known and widely adopted by consumers, they're inherently limited in their utility; if I want to check my credit card balance from my wife's phone, for example, I can only do it if I've enrolled my finger or face print on her device.

The device-based approach also creates security vulnerabilities, including to elder abuse: imagine an unscrupulous adult child, for example, enrolling themselves on an elderly parent's device and then using their face to log-in to (and drain) their parent's bank accounts.

Instead, companies are adopting a server-side approach to biometric authentication, using modalities such as voice biometrics and behavioral biometrics to authenticate customers whenever, wherever, and however they engage—and to simultaneously detect fraudsters no matter the device or identity they hide behind.

Voice biometrics engines, for example, analyse hundreds of characteristics of a person's natural speech and match them against a library of "voiceprints" that are known to belong to customers or fraudsters. The most advanced engines can do this analysis in less than a second, just from the sound of you telling an agent who you are and why you're calling. Once the agent sees that you've been authenticated, they can focus on helping, not interrogating you.

Behavioral biometrics solutions analyse how people type, swipe, use a mouse, and many other factors in their digital behavior. They're ideal for continuous authentication in digital channels, as they can quickly spot sessions that have been hijacked by fraudsters.

Conversational biometrics—the new kid on the fraud prevention block—offers yet another factor to determine if someone is who they claim to be. These solutions analyse the way people construct sentences, the words they choose, or even the emojis they use, making them well-suited to identifying fraud mules using scripts.

Biometric authentication delivers positive outcomes for everyone

The good news for security and fraud prevention professionals is that 50% of the respondents to our survey say they're now more comfortable using biometrics to authenticate themselves than they were before the pandemic. Two in five (38%) say they trust some form of biometrics to authenticate their identity.

Customers value the way biometrics removes friction from engaging with brands, as they no longer have to remember their credentials or go through password reset processes.

By combining biometrics and other authentication factors in a layered approach to security, underpinned

by AI, organisations can assess the risk of any given interaction in real-time. The results are dramatic reductions in average handle times, contact center costs, and fraud losses.

For example, when NatWest Group (formerly Royal Bank of Scotland Group) implemented voice biometrics to protect its 19 million customers, it reduced fraud losses so much that the solution delivered over 300% ROI in the first 12 months of operation.

Building a more secure future

I hope that by the time next year's Cybersecurity Awareness Month comes around, biometric authentication will be even more commonplace than it is today. And who knows, as more enterprises adopt AI-powered, layered fraud prevention approaches to protect their customers, there will come a day when we don't need a Cybersecurity Awareness Month at all.

Tags: Fraud prevention, Nuance Gatekeeper, Biometric authentication

More Information

Do you want to learn more our authentication and fraud prevention solutions?

Discover how Nuance combines biometric authentication and AI fraud prevention through our unified, omnichannel Gatekeeper solution.

Learn more

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek