Customer engagement, Authentication & fraud prevention

Voice biometrics: Five myths that prevent companies from reimagining customer authentication

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

November 14, 2023

We're all familiar with the famous warning from English philosopher John Stuart Mill: "Bad men need nothing more to compass their ends than that good men should look on and do nothing." It's true for individuals, and it's true for the organizations responsible for protecting their assets and accounts. To paraphrase for today, fraudsters need nothing more to achieve their goals than that organizations should look on and continue relying on outdated customer authentication methods.

Why is now the right time to adopt voice biometrics for authentication and fraud prevention?

Because fraudsters have written a playbook to circumvent nearly every other security method. Because today's technology is faster, more accurate, easier to implement, more scalable, and—thanks to the continuous delivery of the cloud—it's improving every day. And because authenticating customers using account credentials, security questions, and two-factor PINs wastes their time, your agents' time, and your contact center budget, and leaves countless people vulnerable to the exploits of organized crime.

We see it play out every day, like the recent hacks at Caesar's and MGM for example. A high percentage of major security breaches and fraud attacks begin with a few stolen personal details and a little social engineering during a 10-minute phone call. With the proliferation of generative AI tools, inexpensive bots, and Fraud-as-a-Service (FaaS) marketplaces, we face a reality where fraud is not only prevalent but scalable and sophisticated.

In this era of pervasive fraud and fragile customer loyalty, what's holding companies back from adopting fraud prevention measures that keep the bad guys out and make it significantly easier for real customers to get the help they need?

Or, to put it another way, if 85% of consumers now say physical biometrics, including voice, are the most trusted and secure authentication method they've encountered, why aren't they the industry standard?

In our experience working with hundreds of organizations around the globe, the reason is a set of outdated assumptions based on yesterday's technology.

Myth #1: It's too hard to integrate voice biometrics into the contact center

Historically, organizations have struggled to implement voice biometrics due to the complexity of on-premises telephony environments, difficulty acquiring audio from calls, legacy biometric solutions with limited connectivity—or some combination of the three.

But much of this complexity stemmed from hardware requirements for passing audio from calls into a voice biometrics system. First, contact centers needed to find the audio signal within their network, then purchase additional routers or session border controllers to handle the load, and, in some cases, reconfigure their entire network. After solving for audio transmission, the organization still needed to solve for integration into their contact center platform to connect incoming voices with claimed IDs and deliver authentication verdicts within the flow of a call. The upshot: many organizations ended up several months into the deployment journey without performing a single biometric authentication.

Thanks to the innovations cloud has brought to the contact center and to voice biometrics, these headaches are no longer an issue. With modern Contact Center as a Service (CCaaS) platforms and cloud-native biometrics solutions like Nuance Gatekeeper, it's as simple as initiating an API call, and the data begins to flow in both directions.

At Nuance, we've invested heavily in adding out-of-the-box integrations with leading CCaaS providers to enable our customers to get started with a few clicks, in virtually any environment. Today, most developers can read the API documentation and be up and running in hours instead of months.

Myth #2: The performance of voice biometrics isn't good enough

Whether due to an early bad experience, anecdotal evidence from peers, or skepticism based on mixed-bag reviews of the dozens of vendors in our market, some organizations still believe voice biometrics aren't ready for primetime. The failure rates are too high. The algorithms aren't accurate enough. It takes too long to enroll and authenticate. There's too much tuning and calibration to make it all work.

If an organization isn't confident it will see positive business outcomes, it isn't likely to replace its current authentication methods, which may seem "good enough."

But in reality, the technology has improved by leaps and bounds in recent years. Thanks to what we're doing with deep neural networks, our voice biometrics are lightning-fast and incredibly accurate, with minimal error rates. Today, Gatekeeper can deliver 99% authentication success rates, from as little as 10 seconds of enrollment audio and 0.5 seconds of authentication audio. We also regularly see customers detecting fraud attempts with 90%+ true positive rates.

This level of peak performance means that not only are voice biometrics a game-changer for the customer and agent experience, but they can also enable truly automated fraud detection, saving organizations countless hours and millions of dollars every year.

Myth #3: Voice biometrics are vulnerable to AI-generated synthetic speech attacks

Using software to clone someone's voice is nothing new. What's new is the explosion of cheap, easy-to-use generative AI tools available to everyone. With a few spare minutes, anyone can create a synthetic version of their voice, or a potential victim's voice, if they can access the necessary audio samples.

At the dawn of this technology, many media outlets sounded the alarm bells against voice biometrics, categorizing them as a vulnerability and even recommending that organizations revert to traditional knowledge-based and two-factor authentication (2FA).

Should this be a reason to delay the adoption of biometric security? Despite the fact that billions of personal data records are for sale on the dark web and NIST hasn't supported SMS as a secure channel for 2FA since 2016, is it possible that legacy verification factors are still worth the gamble? We don't think so.

In fact, we've been preparing for the fight against "voice deepfakes" long before 2023. Nuance has pioneered anti-spoofing technology for nearly a decade, and we're constantly enhancing our core algorithms to protect organizations from the latest threats, including highly realistic synthetic voices. And thanks to cloud, our most effective countermeasures are instantly made available to all Gatekeeper customers.

We conduct regular testing against the latest AI voice cloning and text-to-speech models on the market, and we use a multilayered approach to prevent attacks. In other words, we don't just check to see if an incoming voice sounds close enough to the voice of the customer; we analyze hidden artifacts in the audio that may indicate it's been digitally manufactured or is being played from a recording. To deliver an authentication verdict, our AI Risk Engine incorporates a variety of other important signals about the caller, their voice, the audio signal, and the call itself.

Myth #4: Voice biometrics are too expensive

Cost is a function of complexity. Suppose it takes months of system configuration, professional services support, custom development, and integration to get a voice biometrics project off the ground. In that case, the upfront cost will be high, and the time to ROI will be long—not to mention the cost of ongoing IT maintenance. Add to that the price of a perpetual or term license, and voice biometrics may seem prohibitively expensive for small and medium-sized businesses.

However, the consumption-based subscription model, made possible by cloud delivery, is playing a huge role in driving down costs and eliminating upfront investment for companies of all sizes. You pay for the solution as you use it, based on your level of use. Instead of all the manual development work required to maintain a packaged solution, we seamlessly deliver the latest updates, fixes, and enhancements to your environment.

We've seen countless smaller organizations like community banks and credit unions deploy Gatekeeper to only a handful of contact center agents and achieve positive ROI within the first year. And thanks to improvements in out-of-the-box usability, we regularly see organizations delivering real benefits to customers, agents, and fraud teams in as little as 90 days.

Myth #5: The biggest myth of all

Perhaps the most damaging myth around authentication and fraud prevention is that voice biometrics are a luxury rather than a necessity.

Many contact centers are overwhelmed with volume, under-resourced due to agent attrition, and struggling to advance digital transformation initiatives and fully embrace cloud. Fraud is a constant presence, but no one knows how deep and broad the damage might be, or which holes to patch first.

So, where do you make your investments? Do you take a risk on voice biometrics, or accept the risk you already face with traditional ID&V? Do you reach for AHT savings and improved CX, or accept slow, unreliable authentication as par for the course?

Whatever you decide, don't buy into any of these misconceptions that hold organizations back from massive potential savings and a customer experience that truly feels human. And don't believe for a second that the fraudsters preying on your customers and your business will wait for tomorrow. They hope you keep things exactly the way they are today.

Tags: Security & biometrics, Biometric authentication, Nuance Gatekeeper

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