

# The essential guide to voice biometrics.

---

## Key takeaways

Validating the identity of customers within customer service channels has become a critical component to enterprise security. In this guide, we provide an introduction to voice biometrics technology, real-world use cases across customer channels and three action steps to help you get started.

---

# Table of contents

## **1 Voice biometrics – an introduction / p2**

- What is it, how it works, and is it accurate?

## **2 Voice biometrics – how to use it / p3**






- IVR automated authentication
- Agent assisted authentication
- Mobile application authentication
- Employee authentication
- A unified credential across channels

## **3 Voice biometrics – three steps to get started / p6**

- Align with overall customer service strategy
- Enlist experts with a proven track record
- Plan for cross-channel from day one

## Voice biometrics – an introduction

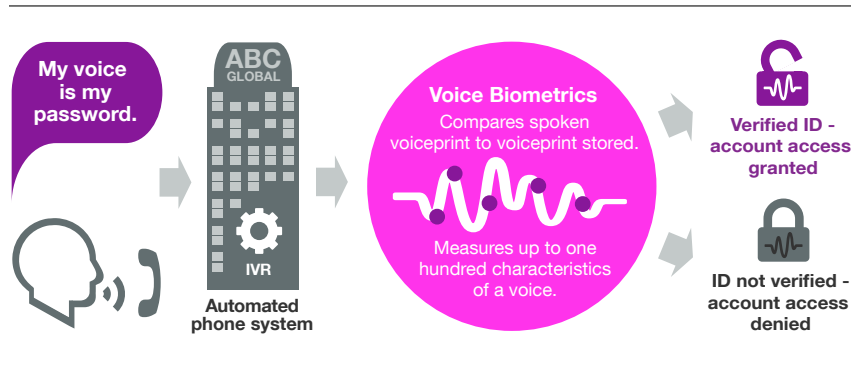
Voice biometrics is a technology that is increasingly being used by organizations around the world that include financial institutions, telecommunication service providers and other enterprises that require validating the identify of customers within customer service channels. Yet the technology and it's wide range of benefits are not fully understood by many. This guide provides an introduction of voice biometrics to allow you to understand what voice biometrics is and how it can be used within your organization.

 <p><b>What does it do?</b> A very simple task that can be quite complex.</p> <ul style="list-style-type: none"> <li>- Listens to a human's voice and determines who that person is.</li> <li>- Distinguishes voice characteristics based on size and shape of the speaker's vocal tract, mouth, teeth and other physical characteristics.</li> <li>- Measures behavioral characteristics such as accent, speaking rhythm and more.</li> </ul> <div data-bbox="245 968 630 1346"> <p><b>Behavioral Factors</b></p> <ul style="list-style-type: none"> <li>Speed of Speech</li> <li>Pronunciation and Emphasis</li> <li>Accents</li> </ul> <p><b>Physical Factors</b></p> <ul style="list-style-type: none"> <li>Unique Physical Traits of Vocal Tract</li> <li>Mouth Shape and Size</li> <li>Nasal Passages</li> </ul> </div>	 <p><b>What is a voiceprint?</b> A stored utterance of a human voice used to verify a person's identity.</p> <ul style="list-style-type: none"> <li>- Captured by voice biometrics software to later identify the individual speaking.</li> <li>- Based on unique physical and behavioral characteristics of our voice.</li> </ul>
 <p><b>How does it work?</b> Uses a voiceprint unique to each person much like a fingerprint.</p> <ul style="list-style-type: none"> <li>- Captures a person's voice typically through the microphone of a phone.</li> <li>- Analyzes a spoken phrase against a stored voiceprint.</li> <li>- Measures up to one hundred characteristics of a voice including behavioral and physical factors.</li> <li>- Uses software algorithms to compare the captured voice characteristics to the characteristics of a previously created voice print.</li> </ul>	 <p><b>Does it always work?</b> Highly accurate but not completely infallible.</p> <ul style="list-style-type: none"> <li>- Uses the voiceprint along with statistical models to determine the likelihood that a voice matches to person registered with a voiceprint.</li> <li>- Depends upon the way the voiceprint is originally captured (microphone quality, background noise, line and compression quality are a few factors that can create distortions).</li> <li>- Consistently and significantly more effective than PINs, passwords, tokens and more, at providing legitimate users access to customer care systems and preventing malicious users entry.</li> </ul>  <p><b>So what about accuracy?</b> Can more than double traditional automated authentication rates.</p> <ul style="list-style-type: none"> <li>- It can be very accurate - in fact a leading financial instituion in the United States has achieved a 99.6% success rate on an annual volume surpassing 20 million voice biometric verifications.</li> </ul>

## Voice biometrics – how to use it

From banks to pizza delivery companies – organizations around the world are using voice biometrics for an easy and secure way to authenticate their customers.

### IVR automated authentication

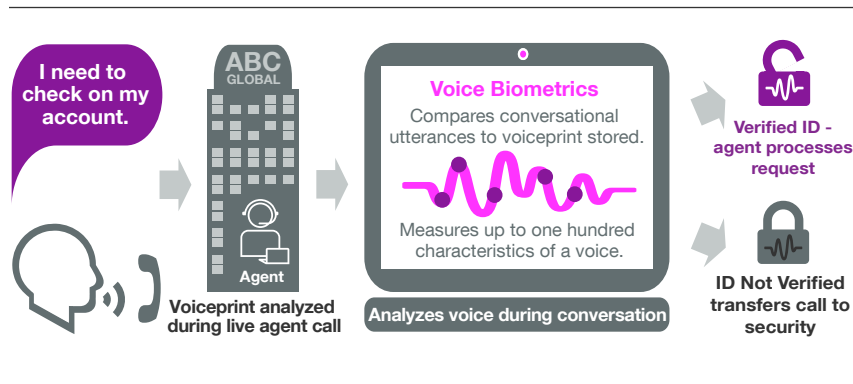


By far the most common voice biometrics application within organizations is the authentication of customers as they dial into the Interactive Voice Response (IVR) system. Typically, customers will be asked to speak a common passphrase, such as "At ABC Global, my voice is my password." Once authenticated, the customer can perform transactions or retrieve information on their account. If the customer chooses to transfer to an agent, they are already authenticated via voice biometrics and the agent can immediately service the customer. There is no additional need for an agent-enforced interrogation process.

One of the main reasons why voice biometrics has been so prevalent in the IVR authentication space, is that the typical authentication method (PINs) is such a poor authentication method from both a security perspective (many people select PINs that are easily compromised) and from a user-convenience perspective (many people forget their IVR PINs as they do not call regularly). With voice biometrics, the return on investment is typically tremendous, as successful automated authentication with PINs is generally low (often in the 30% to 60% range) and fraud committed in the call center is typically higher than in other customer service channels. Voice biometrics can significantly improve the customer experience by making authentication simple, reduce call center costs by keeping callers in the IVR and increasing self-service rates, and by reducing fraud losses by making it more difficult for a fraudster to compromise an account.

Voice biometrics is used today in a wide range of IVR systems - for self-service banking where it secures multi-million dollar wire transfers - to self-service telecommunications for accessing account settings and information.

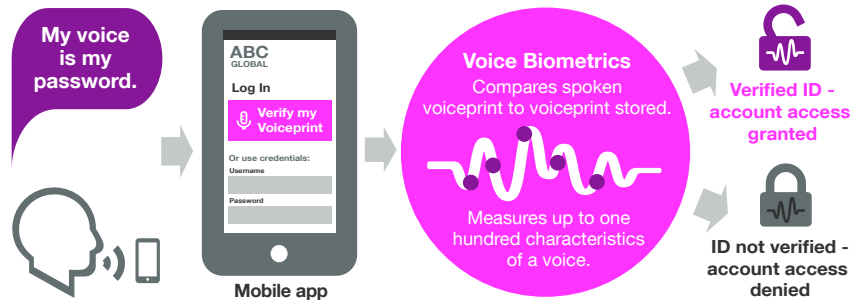
## Agent assisted authentication



Closely related to IVR authentication is the automated authentication of callers when they speak to an agent. In situations where authenticating callers in the IVR is not possible, or desirable, voice biometrics can be used when the caller reaches an agent. However, unlike authentication within the IVR, the caller is not required to speak anything specific to get authenticated. In these scenarios, voice biometrics is operating in a passive mode, listening to a live conversation with an agent and then providing the agent with a confirmation of identity on the agent's computer screen. This form of voice biometric authentication has the benefit of reducing the call handle time as the agent does not need to ask the customer a series of security questions before servicing the customer. Voice biometrics can also significantly reduce fraud as the call center is particularly vulnerable to social engineering and other malicious attacks.

Although the use of voice biometrics by organizations in live agent calls has a less immediate financial impact when compared to automating authentication in the IVR, the implementation of passive voice biometrics is much quicker and requires no effort on the part of the customer. This is becoming increasingly appealing to organizations wishing to deploy voice biometrics to their premium customer segments. For these organizations, delivering an exceptional customer service experience provides the organization with a meaningful competitive advantage that can be measured in customer retention and new customer acquisition metrics. The level of personalization that can be delivered thanks to voice biometrics is comparable to establishing a personal relationship with the customer. For example, agents can answer calls, greeting a customer by name and immediately servicing their request. The customer feels as if the agent knows who they are and that they are valued by the organization. The agent treats the customer without any suspicion of identity and the threat of a fraudster representing themselves as the customer is diminished.

## Mobile application authentication



Beyond the call center, the most significant area of growth for voice biometrics applications within organizations is the authentication of users via mobile applications. Currently, mobile application developers struggle with a basic trade-off. As authentication is made more secure, e.g. by implementing complex alpha-numeric passwords, mobile application usage drops. Typing combinations of numbers, letters and special characters is frustrating and leads to a high failure rate on a SmartPhone device. Initially, the alternative was to implement very weak authentication methods such as a 4-digit PIN or no authentication at all. This limits the functionality that can be offered within the mobile application. Voice biometrics offers organizations an elegant solution that favors usage while enhancing security. Similar to the use of voice biometrics in an IVR, mobile application users can be asked to speak a common passphrase such as “At ABC Global, my voice is my password” to access the application or to authorize a high-risk transaction.

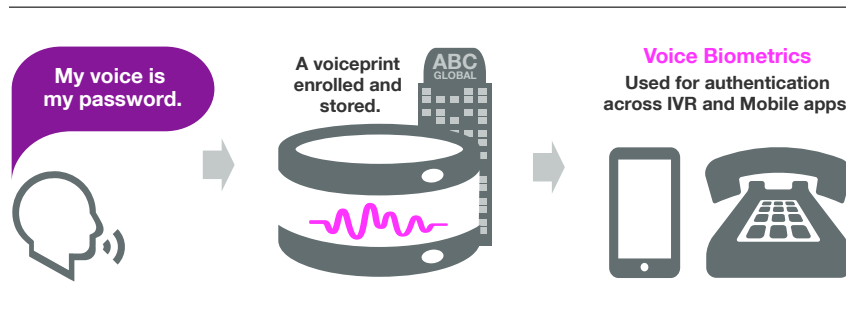
Voice biometrics has helped organizations increase their mobile application usage and enable the number and type of transactions that can be performed on a mobile device. This in turn reduces the load on more costly customer service channels, such as the call center.

## Employee authentication

Authenticating customers is the most common use-case for voice biometrics as a customer-facing solution, but the same technology can also be used to authenticate employees. Many organizations have successfully leveraged the technology for numerous internal applications. For example, voice biometrics has proven to be an effective method of automating the process of re-setting an employee’s Windows password, authenticating employee-to-employee calls and validating employee identity when dialing an internal call center (such as the IT or the HR helpdesk). Organizations are using voice biometrics to secure high-risk transactions performed by employees and authenticating remote employees to work securely within applications.

Although the scale of these deployments is often smaller than the customer-facing applications, organizations can realize significant productivity gains by streamlining the authentication procedures and at the same time reducing internal fraud.

## A unified credential across channels



Once it has been registered using a mobile application or IVR, a person's voiceprint can be used to identify that person in both channels. As such, voice biometrics can unify the often disjointed approaches to authentication that currently exist within internal and external systems. Instead of asking for a PIN in the IVR and a complex alpha-numeric password in the mobile application, the same passphrase "At ABC Global, my voice is my password" can be used to authenticate in both channels. This has helped organizations make the authentication experience consistent for customers, while complying with security requirements.

## Voice biometrics - three steps to get started

**There is no one-size-fits-all approach, but these three steps will give you insight into how you should approach implementation.**

### Step 1

#### Align with overall customer service strategy

This is by far the most important step and failing to clearly align with the organization's customer service strategy will determine the fate of a voice biometrics initiative. A strategy that is weighed towards minimizing costs will typically favor implementing voice biometrics in the IVR as a first step, whereas a strategy focused on delivering a differentiated customer experience will favor beginning with the agent and/or mobile applications. Aligning voice biometrics with the overall customer service strategy will not only enable an organization to make a considered choice for where the first application of voice biometrics will be delivered, but also how the technology will be deployed. As an example, a strategy focused on reducing fraud will dictate a more stringent deployment of voice biometrics by potentially combining voice biometrics with another authentication factor, or asking the customer to speak a one-time password (OTP) instead of a common passphrase. By contrast, a strategy focused on maximizing the customer success rate will instead favor a simple common passphrase and not require any overt additional authentication step on the part of the user.

### Step 2

#### Enlist experts with a proven track record

It is likely that most organizations do not have their own internal voice biometrics experts, unlike IT personnel well versed in traditional PIN and password-based authentication. To ensure the success of an initiative that includes voice biometrics, it is imperative that some reliance is placed on

the expertise of individuals and organizations that have 1) developed the various voice biometrics technologies, and 2) successfully deployed these technologies in multiple situations around the globe. Experience shows that some organizations which have chosen to drive the design and deployment processes independently, have encountered challenges that have slowed the adoption rates of the voice biometrics solution by their customers. It can just as easily relate to limited authentication success rates. Voice biometrics experts should be used to guide an organization, not only in the technical design of the solution, but also in the go-to-market strategy and use-cases that will lift utilization rates and make the enrollment process simpler for customers.

### Step 3

#### Plan for cross-channel from day 1

Even though the initial application for a voice biometrics deployment may be limited to a specific channel, it is highly recommended that the evolutionary plan includes consideration for cross-channel deployment from the onset of the project. Once deployment in one channel is successful, an organization will invariably realize the benefits of the solution and leverage it in additional channels. Having this vision early will ensure that the right technology is selected, but will also ensure that all design decisions are not taken in isolation. This can include, but not be limited to, how voiceprints are collected and the wording of passphrases which can enable one voice biometrics system to be leveraged in a different context. Ultimately, this will minimize the financial impact on an organization, enable a speedy implementation of voice biometrics across the organization and provide a consistent customer experience across multiple customer-facing interaction channels.

#### Why is Nuance the leader in voice biometrics?

With over 55 million enrolled voiceprints and a global customer base that spans all major industries, Nuance has unrivaled experience in delivering successful voice biometric solutions that enable organizations to improve customer satisfaction, reduce costs and improve security.

### Voice biometrics – learn more

For more information about Nuance's Voice Biometrics solutions, please [visit our Web site](#), or email us at [customerexperienceexperts@nuance.com](mailto:customerexperienceexperts@nuance.com).



---

#### About Nuance Communications, Inc.

Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit [nuance.com](http://nuance.com).

---