Voice biometrics FAQ

Commonly asked questions related to Voice Biometrics

Q: What is Voice Biometrics and how does it work?
A: The voice biometrics technology is a speaker authentication technology that captures a voice sample from a live caller, compares it to a previously stored voiceprint, and produces a confidence score of how closely the caller's voice sample matches the voiceprint. A voiceprint includes more than 100 unique physical and behavioral characteristics of a person such as length of the vocal tract, nasal passage, and pitch, cadence, accent, etc. Independent research has shown that a voiceprint is unique to an individual, just as a fingerprint is.

Q: Where are voiceprints stored?
A: Voiceprints are encrypted and stored in a secure database behind the firewall, just like any other sensitive client data. Nuance does not maintain a repository of voiceprints.

Q: What about privacy concerns? Are consumers aware that their voice is being recorded?
A: Nuance's best practice recommendation is for organizations to disclose the use of voice biometrics with its customer. Customers should be aware that voice biometrics is being used, and they should have the ability to opt out of using it should they so choose. What we have learned is that disclosing the use of voice biometrics has helped many of our customers to differentiate themselves in their respective markets. While PINs and passwords continue to fail, and hacks and breaches climb, organizations that are deploying voice biometrics show that they are truly innovating the customer experience, and taking their customers' security seriously.

Q: Can the system be "hacked?" Specifically, what if I recorded your voice, then played it back to a VB system and pretended to be you? Couldn't I fool the system easily in this way?
A: Nuance has several measures in place to ensure that a system could not be breached by a recorded playback of a person's voice. Technologies such as Playback Detection and Liveness Detection are able to quickly flag whether the spoken voice coming into the system is recorded or live, or whether speakers have changed.

Q: What about an impersonator? Or identical twins? Could they easily trick the VB system?
A: There are more than 100 characteristics being measured when it comes to evaluating someone's voice and matching it against a voiceprint – unique to each person. This includes both physical characteristics – the size and shape of the larynx or nasal cavity, for example – and behavioral characteristics – rhythm of speech, intonation, accent, etc. While behaviors can be easily mimicked, physical voice characteristics cannot, and this prevents impersonators or identical twins from "tricking" the system. Nuance has a number of protocols in place to ensure highly accurate matching of a person's voice against their unique voiceprint.

Q: What if I have a cold? Won't the system fail? If the VB system does fail, is there a backup in place?
A: Normal fluctuations in a person's voice won't adversely cause a voice biometrics system to fail. However, if someone has a physical ailment such as laryngitis or a more severe illness which causes an inability to speak, voice biometrics technology will obviously be challenged. In this case, customers

would simply revert to another biometric (if offered), or to a series of authentication questions. This depends on the system being used.

Q: What is the benefit to a customer?
A: The overall objective of implementing voice biometrics is to increase client convenience for authentication and to enhance security. Voice biometrics eliminates the need for PINs, passwords or security questions, and makes it possible for customers to speak a simple voice pass phrase for authentication.

Q: How secure is it?
A: Voice biometrics technology can be used as a multi-factor authentication method (something you know, which is the passphrase, and something you are, which is your voice). The security is among the strongest in the industry. Voice biometrics technology is less susceptible to fraud threats that affect more traditional methods of authentication such as PINs and passwords.

Q: With the voice biometrics system that is in place, is it possible for somebody else to be falsely accepted on my account?
A: There is no biometrics system or security system that is 100% fool-proof. While extremely rare, there is a minute possibility of a voice biometrics system falsely accepting an incorrect speaker for the true speaker upon multiple attempts, under very certain circumstances (for example, in the case of an identical twin where the siblings have nearly identical physical characteristics). The chances that a false accept will occur with a genetically related relative of a similar age and of the same gender is much higher than a false accept with a random stranger, and this probability is heightened with a twin. This issue is present with all biometric factors, and is not unique to voice biometrics.

Q: How can you prevent someone being falsely accepted into my account?
A: To prevent these "false accepts," we have many layers of security that act in tandem with voice biometrics, such as requiring an additional piece of personal information, as well an industry standard security practice to lock accounts after two or three failed access attempts. Additionally, leveraging multiple layers of security, especially for high-risk transactions, is another best practice.

Q: Shouldn't voice biometrics be able to identify each and every person as unique? If there is even a remote chance of a "false accept," isn't it risky to use voice biometrics?
A: We've seen PINs, passwords and security questions lead to massive-scale data breaches at some of the largest organizations in the world. Time and again, passwords are stolen and massive amounts of data are compromised, putting consumers at risk. Today's voice biometrics have proven to reduce security risk and to drive down fraud, while at the same time offering a more convenient user experience.