TRANSAMERICA®

Transamerica Voice Pass FAQ

Frequently asked questions related to Transamerica Voice Pass, a voice biometrics system

Q: What is voice biometrics, and how does it work?
A: Voice biometrics 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 voice characteristics 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: 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: What is the benefit to a customer?
A: Enhanced security and convenience. 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: Where are voiceprints stored?
A: Digital representations of the 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: We give our customers the option to enroll in Voice Pass and let them know exactly what's involved if they do. If they decide against it, opting out is easy.

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 voice matching.

Q: What if the customer has 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 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 the event that the voice authentication fails for any reason, the caller will be transferred to a CCR, who would authenticate and then provide service.