VoiceIt
YOU ARE KEY®

AN OVERVIEW OF VIDEO BIOMETRICS

WHO WE ARE

VoiceIt is comprised of forward-thinking individuals, fostering innovation to remain an industry-leading Voice Biometric security provider.

WHERE WE ARE

Though we have a global network, we are happy to call Minneapolis, MN our home.

As passwords and MFA have proven to create issues with the average user, we have focused our efforts on providing a frictionless user experience that provides the latest advances in security across telephony, mobile apps, and web browsers.

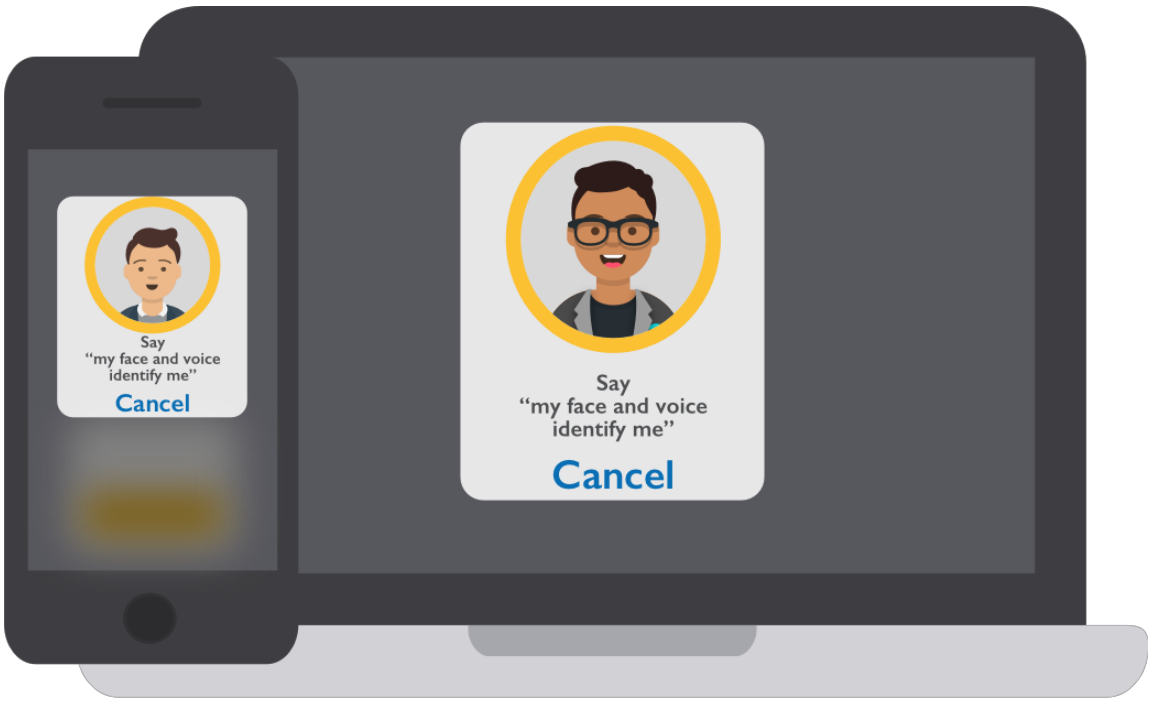
About VoiceIt

VoiceIt Technologies has been a trailblazer in the voice biometric field since providing the industry's first online voiceprint portal with cloud-hosted services in 2007. Along this journey, **VoiceIt** has integrated its top of the line Video (Face + Voice) Biometrics in order to reduce fraud and increase security stability within companies of all sizes.

VoiceIt prides itself on providing a great experience by focusing on individualized customer-facing experiences and unique services. This white paper will explore what **VoiceIt** has to offer and enforce the idea that the **VoiceIt** Video (Face + Voice) Biometrics platform, is a critical part of creating a secure and dependable partnership.

What is Video Biometrics?

Video (Face + Voice) Biometrics is an integrated multimodal and multiengine identification and verification solution. Providing advanced Multi-Factor Authentication (MFA) security in a simple-to-use format with minimal friction. With SDKs available for Android, iOS, and Web Browsers, users are able to access Video (Face + Voice) Biometrics without the need for specialized hardware.



How does Video Biometrics work?

The Video Biometric Verification process is made up of two simple steps:

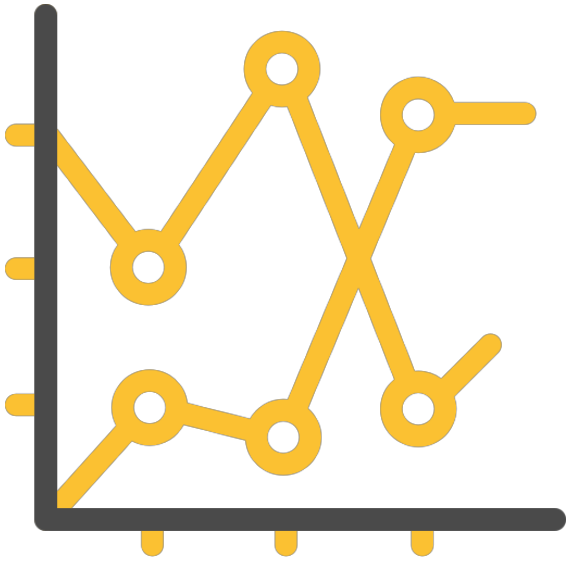
1. Enrollment - The creation of the voiceprint and face profile
    - The enrollment process consists of capturing 3 video (face+voice) recordings with a user speaking a Voiceprint Phrase

- These 3 video recordings are used to create facial enrollments and voice enrollments
- After a user enrolls via the video enrollment method, they have the ability to perform verifications with face, voice, or video (face+voice)

2. Identification (1:N) or Verification (1:1) with Liveness Detection
    - The user will be prompted with the Liveness Detection
    - The user will capture their face and voice in a video recording including the Voiceprint Phrase
    - Identification (1:N)
        - Meant to be used with a subsequent Verification
    - Verification (1-to-1)
        - Used to authenticate and verify the identity of an individual

What are Risk Thresholds?

Risk Thresholds have been modeled for Video (Face + Voice) Biometrics to allow for extended usability in low-quality audio or visual surroundings. Liveness Detection (available in the Android, iOS, and Web SDKs) is a key variable used in the calculation of Risk Thresholds. When Liveness Detection is implemented, a lower Risk Threshold is available as the risk of a replay attack is exponentially lower. Other variables used to calculate Risk Thresholds include, but are not limited to: use case, confidence settings, and channels used.



What is Multi-Engine Analysis?

Why verify once when you can verify multiple times simultaneously?
Check, double check, and check it again. That is how **VoiceIt** views biometric engines. With each engine having its own strengths and weaknesses, **VoiceIt's** unique multi-engine approach provides an unparalleled experience of both usability and security. To ensure maximum performance, all biometric engines are developed and updated by an in-house team of engineers and researchers.

What is Liveness Detection?

Liveness Detection is comprised of simple actions such as looking left/right, smiling and blinking. When used in a randomized order, they provide protection from replay attacks using photos and videos.

What kind of accuracy is expected?

When making a decision regarding Biometrics, there are two main statistics to be aware of: **False Acceptance Rate (FAR)** and **False Rejection Rate (FRR)**.

False Acceptance Rate (FAR) is the measure of the likelihood that the biometric security system will incorrectly **accept** an access attempt by an unauthorized user.

False Rejection Rate (FRR) is the measure of the likelihood that the biometric security system will incorrectly **reject** an access attempt by an authorized user.

VoiceIt is proud to provide customers with a **FAR of 0.0001%** complemented by a **FRR of 1% - 10%** depending on the Risk Thresholds used.

What is Personally Identifiable Information?

Personally Identifiable Information (PII) is any type of information that can be used to identify a user, such as an address, name, or phone number. With privacy built into **VoiceIt's** DNA, there is no need to input PII into the system because the system will autogenerate universally unique identifier (UUID) for every user enrolled.

About **VoiceIt**

VoiceIt provides a (Patented) cloud-based, pay-as-you-go, face and voice biometrics platform that allows for rapid development and deployment of security solutions. Whatever the integration needs, **VoiceIt** removes traditional industry obstacles by providing a secure platform at a reasonable cost.

Centered on privacy and security, all features have been built to ensure the security and stability of the system are safeguarded in any deployment environment.