

# PASSIVE Voice Biometrics in ACTIVE channels

## The change that will spearhead large-scale adoption of voice biometrics

By Ravin Sanjith, Program Director Intelligent Authentication, **Opus Research**

Speech processing has enjoyed incremental improvements for quite a while; most recently in the evolution from Automated Speech Recognition (“ASR”) to Natural Language Understanding (“NLU”). As scientists continually devise methods to enhance biometric template creation and pattern matching, more recent innovations in machine learning and artificial intelligence are yielding an ever-increasing spread of classification metrics, especially in Voice Biometrics (VB), through the virtuous cycle of ongoing machine learning from more and ‘bigger’ data.

Initial VB implementations mainly involved text-dependent speaker authentication, referred to as “active voice biometrics”, which when combined with ASR yielded better results than text-independent or (PASSIVE) VB. Today, thanks to significant technology advancements, PASSIVE authentication is used to deliver a highly accurate, in a more seamless customer experience.

Traditionally, implementations of text dependent versus text independent solutions were quite distinctly aligned with self-service implementations versus human-assisted channels, respectively. Hence, in most deployments, ACTIVE VB takes place in IVR and/or digital (e.g. mobile) channel, while PASSIVE VB applies to agent-on-phone interactions. But that is changing.

### ACTIVE voice biometrics calls for user-specific behavior

Text-dependent VB, as the name suggests, depends on a specific or anticipated utterance, known as a ‘passphrase’, for which a wide range of options exist (see insert). As with all biometrics, users need to enrol first in order to verify as and when needed.

**ENROLLMENT** involves 2 components:

- **Identity assertion**, also referred to as ‘Ground Truth’, is an essential part of the enrollment process; most common for Contact Centres is the use of existing authentication mechanisms, mainly security questions or “KBA” (knowledge-based authentication) as it is more commonly known.
- **Voiceprint creation** is achieved through collecting a number of utterances, usually 3, to accommodate for natural variances in speaker responses.

**VERIFICATION** is performed when the caller repeats the relevant phrase at least once, and this is compared to the enrolled voiceprint for a match/mismatch decision.

The VB process for ACTIVE enrollment and verification requires very specific user behaviors, and has often been cited as the root cause of caller abandonment from voice authentication; purportedly due to the cognitive load, mental effort, or more simply put, demands on the caller to concentrate on unfamiliar IVR instructions, especially if in a hurry or while multi-tasking.

### Examples of Text Dependent Passphrases

- **Common** - where all callers are prompted for the same response (e.g. “I am using voice biometrics”)
- **Random** - typically a fixed set of phrases that could randomly prompted, also used to detect ‘liveness’ (e.g. “The best things in life are free”)
- **Dynamic** - similar to ‘random’ but generally uses short (4 to 6) number sequences (e.g. “3,7,4,8”)
- **Individual** - where a user is prompted to say their name or social security number; and is generally static per user (e.g. “AAA345CZ5”)

## Machine Learning is blurring the lines between ACTIVE and PASSIVE voice biometrics

The application of machine learning methods have yielded massive improvements in both accuracy and speed of response for biometrics in general; but for voice biometrics this is a quantum leap! Less net caller audio is required to yield similar, if not better, accuracy. More specifically, where older-generation text-independent solutions typically required at minimum 6-8 seconds of net audio, they are now capable of providing adequate results within 3-5 seconds; this is generally within the length of text-dependent vocal responses.

Practically, what this means is that a spoken response, prompted by a speech-enabled IVR (or even a mobile screen prompt) may be long enough to gather adequate net audio to verify a caller without a specific passphrase.

**The real game changer -- and this really is a game changer -- is that a single voiceprint may be used for both ACTIVE and PASSIVE verification.**

## Conversational responses in IVR and digital channels will spearhead large scale adoption

ACTIVE/text-dependent and PASSIVE/text-independent technologies are still regarded as being distinct and independent of one another. However, we are at the cusp of a revolution. As text-dependent and text-independent technologies meld into a single CONVERSATIONAL RESPONSE, the terms of ACTIVE and PASSIVE will no longer refer to the underlying technology. These terms may still remain in use, but will apply instead only to user behaviour, and even that may disappear as consumers voraciously increase their demand to seamless, frictionless and continuous experiences... but that topic is for a different note.

Furthermore, the promise of a single voiceprint will also drive further innovations in sharing and federation; a topic receiving growing attention in Identification & Verification regulatory circles, as well as immense momentum in collaborative fraud-mitigation.

Opus Research has always been a strong proponent of Voice Biometrics, and since early 2000 has witnessed immense technology improvements, however with adoption somewhat lagging; and one of the main causes is the trade-offs between text-dependent and text-independent capabilities, and the negative impact on enterprise integrations as well as user experience. This is especially evident in large contact centers where both self-service and agent-assisted authentication is required. Their blending into a single function brings enormous infrastructure and data efficiencies, and most importantly, a more seamless and frictionless customer experience. We are very impressed by the immense investment being made by vendors such as NICE taking this approach and applying Passive to Active channels which will be the tipping point for unlocking truly large scale adoption, globally.

## Program Director: Intelligent Authentication Opus Research



**Ravin Sanjith**  
B. Sc. Engineering  
B. Comm  
MBA

### Biography:

Ravin possesses a blend of technical and commercial acumen, accumulated over 25+ years across a multitude of industries and disciplines.

Ravin started his career in 1992 as an Engineer in the Energy industry, followed by more than 10 years in the Financial Services field. He spent the next decade in a range of technology startups as partner, founder and general intrapreneur. After holding C-level positions in various industries, Ravin started his own consulting practice in 2010; where he took an interest in the use of biometrics to curb ID&V security and customer experience challenges. He then co-founded OneVault, a global pioneer in delivering Voice Biometrics. Most recently he has joined Opus Research as Program Director: Intelligent Authentication.

Ravin holds degrees in Engineering and Commerce, as well as an MBA.