ValidSoft Trusted eXperience™

Voice Identity Assurance for Contact Center, IVR/IVA and all Customer Engagement Channels

Deliver Trusted eXperiences using secure voice biometric identity assurance regardless of channel

Delivering Trusted eXperiences is a business imperative

The growth in digital channels and the ways in which we communicate and transact with our suppliers and providers on a daily basis is an evolving journey. The physical branch evolved into a website which spawned a smartphone app and now embraces home digital assistants via a smart speaker. The pandemic dramatically speeded up the evolution.

Many organizations no longer have offices or branches to visit even if we wanted to. "In person" queries and requests are handled via remote contact centers and interactive voice response platforms, whilst websites and apps service their customer through chatbots, speechbots and intelligent assistants.

Contact Center fraud is growing unabated, and account takeover losses associated with contact centers reached $775million in 2020
Source: Aite Group

Knowledge Based Authentication (KBA), pervasive in the contact center, is fundamentally compromised

Central to this core issue across these channels is the need for identity assurance in order to prevent the genuine customer becoming a victim of an account takeover, fraud or identity theft.

Consumers need to feel confident that organizations employ strong security protocols and procedures to protect their privacy, personal data and assets, but equally expect the experience should be frictionless, consistent and expedient.

However, the way many organizations verify identity is a hotchpotch of methods that aren't very secure, provide a poor user experience and don't suit the channel on which they are deployed.

Knowledge-based authentication (KBA) in the contact center provides a poor user experience that can lead to call abandonment or denial of service and is incapable of protecting against hackers and fraudsters.

Passwords, PINs and other weak forms of identity assurance have all been long broken and offer little in the way of confidence to consumers.

What do users want?

- A fast, easy-to-use, reliable and expedient method of identity assurance
- A consistent experience across all contact points
- Predictability when contacting organizations
- No questions and answers and no requests for personal information
- Trust they won't fall victim to account takeover or fraud

It is estimated staff will continue to work remote or distributed 50-100% of the time for the foreseeable future creating an ongoing opportunity for hackers and fraudsters.

Source: Independent research

What are the benefits of voice identity assurance?

1. Fast, frictionless identity assured authentication
2. Reduced abandonments due to inability to answer Knowledge-based Authentication
3. Improved customer satisfaction
4. Reduced fraud across all channels
5. Reduced cost
6. Ability to deploy across all consumer touch points

Consistent and predictable Voice Biometric identity assurance provides a trusted user experience regardless of channel or contact point.

Enter **ValidSoft Trusted eXperience™**

Based on the consumer's voice, Trusted eXperience provides a single form of identity assurance that is fast, frictionless, consistent, predictable and repeatable on all channels.

Using ValidSoft's world-leading voice biometric technology, Trusted eXperience integrates with web browsers, apps, IVR's, IVA's, speechbots, and contact centers to provide consumers with real confidence that their identity, and personal assets, are taken seriously.

As voice continues to gain traction as the user interface of choice, across multiple channels, using voice is the most transparent, fastest, most secure and convenient way for consumers to self authenticate.

With nothing to remember and nothing to forget, Trusted eXperience is the easiest and most secure user experience for identity assurance in an omni-channel world.

THE FASTEST MOST ACCURATE VOICE BIOMETRICS TECHNOLOGY ACROSS ALL CHANNELS

Active authentication at the IVR/IVA/LOGIN

"Please authenticate me, with my Voice"
"Please authenticate me with Access Code 123456"
Or simply "123456"

Net speech ~ 0.5 to 1.5 seconds
Elapsed ~ 2 to 3 seconds elapsed

Passive authentication with Agent

"Good morning, I'm calling to check….."
"Hi there, my name is…….."

Net speech ~ 2 to 3 seconds
Elapsed ~ 4 to 6 seconds

…followed by continuous authentication

How it works

Step 1	Step 2	Step 3	Step 4	Step 2
User speaks	Raw audio received	Key features extracted	Model built	Voice print created (no pull)

Did you know?

Your voice is significantly more secure than other forms of biometrics including facial and finger?

This is because your voice provides both behavioral and physiological information as well as being two-dimensional, able to convey context (what is being said) along with the biometric information (who is saying it)

Key Features

Precision Biometrics
What was said + Who said it

Active & Passive
Conversational | Fixed Phrase | Digits

Accurate Anti-spoofing
Replayed Audio | Synthetic Audio

Language Independent
Language Agnostic Technology

Utterance Verification
Extensive Quality Measures

Identify & Authenticate
Customer Authentication | Speaker Identification