validsoft

Using Voice Biometrics to secure the Omni-channel Ecosystem

A White Paper discussing the omni-channel strengths of Voice Biometrics in delivering high trust, low friction authentication to the connected ecosystem.

Contact ValidSoft

UK Office:
30 Moorgate
London EC2R 6JJ
United Kingdom

USA Office:
100 Pearl Street
Hartford, CT 06103
United States of America

Email
request@validsoft.com

Phone
+1(888) 392-0230

Confidentiality and Disclaimer

This document may contain references to information that has been obtained from sources believed to be reliable. ValidSoft does not guarantee the accuracy, completeness or adequacy of such information, and shall have no liability for errors, omissions or inadequacies. The recipient assumes sole responsibility for the interpretation and use of this material for its intended results. Predictions and forward-looking statements in this document reflect current expectations concerning future events and are subject to risks and uncertainties, many of which are beyond the control of ValidSoft. ValidSoft undertakes no obligations to update these statements as a result of new information. Opinions expressed in this document are subject to change without notice.

validsoft

Contents

Omni-Channel Environments

The world has changed, the way customers interact with Enterprises offering them services has diversified and digitised. The ubiquity of mobile and smart devices has presented opportunities and challenges in not only delivering services, but also in securing them. We all live and work in an omni-channel world where communication occurs via telephones, apps, browsers, chat, and any number of connected devices. Who and what we interact with is also varies, from traditional human interaction to AI-driven BOTS. So, while we expect the flexibility of choosing our most convenient communication channel, so too should businesses expect the flexibility of knowing who they're dealing with, regardless of the communication channel or type of business.

Biometric authentication is increasingly being adopted as the identity verification solution of the future. Different organisations have experimented with a number of biometric modalities, including fingerprint, face, iris, vein and voice amongst others. However, within an omni-channel environment, not all modalities can provide an omni-channel authentication solution which delivers a consistent customer experience.

Voice Biometrics offers a natural **high trust, low friction** experience.

In a typical banking environment, for example, customers could interact with a web-portal, a smart-phone app, a menu driven IVR system or the traditional contact-centre. Each of these present different security vulnerabilities and customer experiences. Increasingly, banks are also looking at replacing text-based interaction (chat) with voice-based solutions via AI-driven speech BOTS. This is occurring not only on apps but also home assistants; spoken command-driven devices that are being utilised as a banking channel.

Only Voice is Truly 'Omni'

Imagine a world where there were no PINS, no passwords and no security questions. Where customers could interact and authenticate securely with their service providers in a consistent and frictionless manner. Of the channels described above, only voice can deliver a true omni-channel experience through biometric authentication. Other biometric modalities, i.e. fingerprints, face and iris, can't be used when ringing the contact-centre, interacting with an IVR or talking to a BOT or home assistant. Consistent, expected behavior is what customers require when verifying themselves and what enterprises require to protect themselves and their customers. Having a biometric experience using an app but reverting to inefficient and frustrating Knowledge Based Authentication (KBA) when ringing the contact-centre does not provide the consistency, customer experience or security required by the modern digital world.

Dynamic by Nature

Another feature of voice, unique within biometric modalities, is that it's a dynamic biometric compared to the static nature of other physical modalities. In the event of data leakage, you cannot change your fingerprint, face, retina, or iris. If these biometric features are spoofed through a data leak then the security of the target system or platform is irrevocably broken.

Voice, however, is dynamic, meaning we can speak anything. Simply deleting compromised biometric models and replacing them with a different phrase would ensure the failure of any spoofing attempts. ValidSoft's voice biometric technology also includes inbuilt, passive detection of spoofing, whether through recordings (replay) or synthetic voice. Being passive, this doesn't require the user to do anything apart from speak, as distinct to intrusive methods such as blinking or moving your head.

Security and Convenience Are No Longer Inversely Related

Customers require simplicity in their security mechanisms and customer engagement channels, whilst Enterprises require security and strive for simplicity. Historically where security is concerned, there has been an inverse relationship between customer friction and the strength of a security model - as you increase security, you decrease usability. Voice biometrics, and the versatility it provides, has enabled the potential to approach the application of user authentication and identification differently, delivering high trust (strong security) and low friction. Of the other physical biometric modalities, all are "active", meaning the user must do something, whether it's pressing their finger or fingers on a reader or taking a photo of themselves. These active actions, whilst permitting the authentication to occur, don't serve any other purpose. Given the user is intending to access some information or execute some transaction, they are therefore injecting friction or intrusion into the business process.

Ubiquity, **digitisation** and **access** are driving the intelligent multi-channel experience – omni-channel is a given.

Whilst voice biometrics too can be used in an active mode, it can also be used in a passive mode, meaning it is not apparent that an authentication is even occurring. The key difference is that the authentication is also performing the required business function at the same time. Asking Alexa, for instance, to transfer money to another bank account, is both the transaction and the authentication.

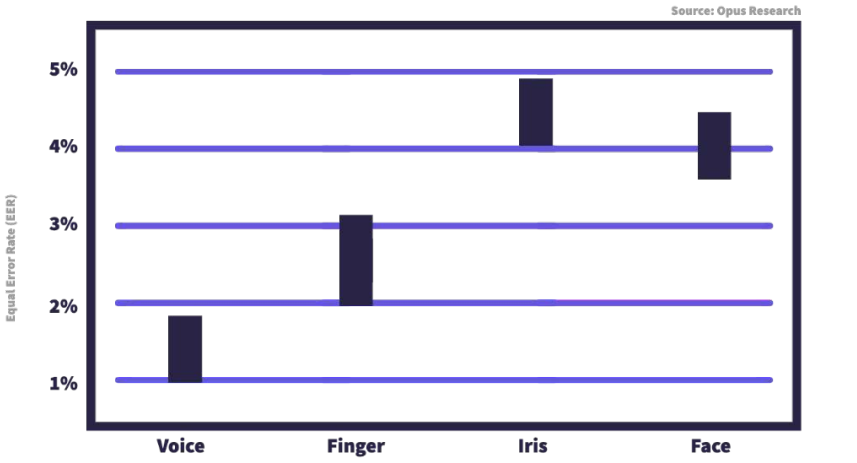
Speaking to a contact-centre agent to arrange a loan is simply fulfilling the customer's needs, whilst authenticating at the same time. There is no friction or intrusion being added to the business process, it is simply leveraging the existing spoken commands or requests. This passive mode of authentication can be implemented on any channel, from apps to call-centres.

Once authentication is applied in this passive way, the process of user authentication no longer occurs at a point in time, it is occurring all the time. As you interact with a chatbot or home assistant, you are passively being authenticated and the context and environment of your transactions is being 'understood'.

Delivering Accuracy and Convenience

The graph below (data from Opus Research) shows how voice is far superior to other modalities in terms of accuracy. The Equal Error Rate (EER) is where the False Acceptance Rate and False Rejection Rate intersect.

Comparing Biometric Modalities; Accuracy



*These are general industry figures and do not apply directly to ValidSoft's technology. We would expect to outperform the generalized industry performance in almost all use cases, particularly where our algorithms are turned to the specific context and application

Voice is the key to **freedom**, **security** and **convenience**

Not only is voice far more accurate than other modalities, it is also far easier to use when performed actively and invisible, in fact, when used passively. No other biometric modality can achieve this degree of accuracy and usability. No other biometric modality can be applied to a diverse set of user engagement channels consistently. Whilst multi-modal (e.g. voice and face) implementations are possible, fusing the biometric modes together, we believe the superior accuracy rates and usability of voice alone far outweigh any marginal security gains that might be achieved, given the friction and intrusiveness that would be introduced.

Why ValidSoft?

We Understand Security

ValidSoft is an industry leading security solutions provider, operating at the intersection of telecommunications and cyber security. Our pedigree is as a multi-factor authentication and security solutions provider and we have spent many years understanding the complexity and subtleties of cyber-fraud, particularly as it applies to payments in the online and mobile worlds. ValidSoft is unique in the Voice Biometric market in that it is not solely a Voice Biometric provider but a security company with an omni-channel, multi-factor authentication platform of which its proprietary Voice Biometric engine forms but one factor.

We Invest in the Future

All of ValidSoft's technology is proprietary, enabling us to specifically tune and tailor our solutions to the context and application of use. ValidSoft recognises that the fraud and security landscapes evolve rapidly, as does technology and how Enterprises apply this

technology to their customer services. To deliver value to our customers, we must continually innovate and be forward-thinking in our approach to the security solutions and technology we offer and invest in. ValidSoft's voice biometric technology has not evolved from a traditional contact-centre offering, built on cumbersome integrations, dedicated on-premise appliances and long-duration conversations. Rather, it has been built with smart devices and smart services in mind, high-definition audio, short-duration passive speech, simple REST-based APIs and an architecture that supports cloud deployments, whilst still being able to be installed on-premise.

Our voice biometric engines also integrate with our User Authentication platform, meaning we are not a binary, one-size-fits-all solution. We can utilise real-time contextual information, use multiple, dynamic thresholds, provide workflow and logic can that can invoke step-up/step-down authentication, support transaction verification and dynamic linking (PSD2) and a user-centric, single biometric template model that is essential in an omni-channel ecosystem.

We Ensure the Privacy of our Customers

Since ValidSoft was founded we have understood the importance of data privacy and adopted a privacy by design approach at the inception of our products. ValidSoft is the only security company in the world that has obtained four European Privacy Seals from the EU. These seals relate to our solutions, and how we control, manage, process and store sensitive data within them. The EU Privacy Seals ensure our products are in complete compliance with General Data Protection Regulation (GDPR) and we have demonstrated compliance with leading global jurisdictions including: US, Brazil, Mexico, China, Russia, Australia, South Africa.

As recent events have demonstrated, enforcement of data privacy is paramount in gaining and maintaining customer confidence. Ensuring customers not only feel they are secured by using our services but also that they, and their sensitive data, is secure when using the service is an important element of this.

We Have a Proven Track Record

ValidSoft have been delivering security solutions into Government, Financial Services and Global Enterprise industry verticals for many years. To enable this, ValidSoft and ValidSoft's security solutions have undergone many external evaluations to ensure the performance and security of our solutions are industry leading. This includes external accreditation by **internationally acclaimed cybersecurity laboratories** and extensive data privacy compliance investigations by **EuroPriSe**. ValidSoft presently provide cyber-fraud prevention solutions to **two of the four Tier 1 retail banking institutions in the UK**, with over **20 million** customers under management. We also secure call centre solutions in major enterprises, including one of the **largest global mobile telecoms operators** with a combined 640 million global subscribers. In addition, ValidSoft provide employee access (remote access) security solutions to **major global enterprises** (FTSE 400) and **government enterprises**.