

Virtual Queuing and Voice Biometrics

Problem

A virtual queuing system educates and empowers customers with respectful options for managing wait time. Rather than wait on hold, the system can put a virtual placeholder into the queue to save your place in line and call you back when it is your turn, in the time promised. Before entering the virtual queue, customers are routed through an IVR where they are authenticated and receive self-service options. When the customer cannot serve themselves, the IVR system classifies their requests based on customer input and then routes them to an agent who possesses the proper skill set to handle the request. The call, as well as the account data of the authenticated customer, is passed to the agent and their screen pop client.

In a virtual queuing scenario, the account data will be passed to the agent as well, once the callback recipient answers the phone and confirms that they are ready to speak to an agent. However, a potential security issue exists when the authenticated customer does not answer the callback. If any other person besides the originally authenticated customer answers the callback, they will be transferred to the agent along with the original customer's account data and create the ideal opportunity for identity theft. This is particularly important in the finance and healthcare industries where reviewing and updating private personal data is inherent to the transaction taking place; the callback could potentially be exploited for monetary gain by an imposter. Risk is low or non-existent in other industries where the nature of the transaction is not personal, such as in the electronic device industry where people do not need to convey personal data in order to receive technical support. Their device may contain private and personal data, but the manufacturer does not need it in order to serve you.

To guard against identity theft in virtual queuing scenarios in the finance and healthcare industries, customer re-authentication is required after the callback has been received by the called party to ensure that the system has positively reached the originally authenticated party from a few minutes prior. Once re-authenticated, the call may now be transferred confidently to an agent along with their personal and private account data. However, to re-authenticate the customer using the original IVR input process would be cumbersome, time-consuming and inconvenient. Therefore, a more streamlined, but highly reliable system is necessary in order to positively confirm identity. It must be operationally efficient, provide a simple process for customers, and most importantly, be secure and accurate.

Technology

Voice biometrics technology relies on the fact that no two human voices are alike. By analyzing the voice pattern of a specific speaker and comparing it with a pre-enrolled voiceprint, which is a statistical model representing the distribution of a speaker's voice biometric features, the technology enables quantifying the similarity between them, pro-

ducing a score which is proportional to the likelihood that the voice indeed came from the speaker whose voiceprint is on file.

Recent advances in classification and machine learning algorithms have led to a significant improvement in the verification accuracy of voice biometrics technology. Independent third party benchmarks conducted by leading research institutes in Europe (CCIR), US (NIST) and Asia Pacific (University of Canberra), indicate an improvement of approximately 50% in verification error rates in the last couple of years.

Today, it is reliably used by financial services, telecom operators, healthcare service providers, and large enterprises worldwide for a variety of employee and customer facing applications. Governments are using the technology to fight crime and terror, as well as to provide an efficient and convenient service to citizens. Studies show that customer acceptance is exceptionally high when compared to other verification methods.

Voice biometrics is a very flexible technology that can be applied in multiple ways. It can be adjusted or tightened to accommodate for a specified security level (false acceptance rate) on the expense of higher false reject rate and vice versa. The Technology can be used to authenticate a speaker during an interaction with an IVR or be deployed in the background of natural conversation.

Successful large scale customer facing voice biometrics deployment, such as the one implemented at Bell Canada in 2008, are paving the way for mainstream use. With 1.5 million voluntary customer enrollments, averaging 100,000 a month, and millions of successful verifications Bell's deployment marks a milestone in this industry – proving ROI and customer acceptance. Dozens of other key large scale deployments across 5 vertical markets and 5 continents are gradually making voice biometrics the ubiquitous way for authenticating people.

Solution

Callers go through an elaborate process today in a company's IVR in order to confirm identity so that their account data can be reliably associated with them when they are transferred to an agent. However, once a customer enters a virtual queue and disconnects from the line, we can no longer trust this customer-to-account data association because the chain of continuous communication has been broken. However, with voice biometric technology we can accurately identify that the callback recipient is indeed the same person who we positively identified as a customer a few minutes prior to the callback. The new inbound IVR process would change slightly to include a step that creates a unique customer voiceprint, similar to a fingerprint. This is accomplished by asking the customer to say a simple pass-phrase, such as "three-five-seven-nine-seven" or "my voice is my password" that contains a wide degree of vocal variance and at least two seconds of net speech. The pass phrase can be constant or variable. This offers no inconvenience to the customer and may be preceded by a prompt that says, "so that we may confirm your identity upon receiving your callback, please say the pass-phrase..." Customers who refuse, will not be allowed to enter the virtual queue, but will be transferred to the physical queue to wait on hold where the communication chain is not broken before reaching an agent.

The voice biometrics system processes the enrolment utterance and, following a feature extraction process, builds a mathematical model which represents the way the specific speaker is pronouncing the selected phrase. The numbers representing this mathematical model are called a voice template.

When the virtual placeholder is next in line to be answered by an agent, it will trigger the virtual queuing system to automatically launch the callback. When the callback is answered, an IVR will prompt the called party to, "please say the pass-phrase 'three-five-seven-nine-seven' so that we may perform a voice biometrics identity match for... [play the .wav or .vox file that is the customer's recorded name]." When the customer says the pass-phrase, the voice pattern is matched against the voiceprint created for this customer just a few minutes ago. If there is a positive identity match, the call is transferred to the properly skilled agent along with their personal screen-pop data that was being temporarily stored in the memory of the virtual queuing system. Upon successful transfer, this data is deleted from the memory of the virtual queuing system. If the voice identity match fails, meaning there may be an imposter on the line, the call is not transferred to an agent with screen-pop data. Instead, this situation may be handled with one of two process methods depending upon your security policies:

- Play a prompt indicating there is a failure to confirm identity. Allow a set amount of retries before finally disconnecting.
- Transfer the call without the screen pop data, at which point, the agent will have to re-authenticate the caller with a series of questions.



USA: 877.886.8187

Europe: +420.222.713.557

Australia: +61.2.8061.7060

Latin America: +52.55.5340.1990

137 Heritage Woods Drive

Akron, Ohio 44321

www.VirtualHold.com

TRY A DEMO 1.888.412.2214