

Your Voice is Your Key

Voice Authentication's Appeal in Multifactor Authentication



relationship management

Your Voice is Your Key

Voice Authentication's Appeal in Multifactor Authentication



By Nancy Jamison

Principal Analyst, Jamison Consulting

Introduction

Personal security and privacy, while always an issue in people's minds, took a huge leap in focus just after 9/11, from both a physical and intellectual property perspective. In the almost decade since that horrific event other events have occurred that have acted as accelerants in the awareness and acceptance of biometrics, including a significant increase in identity theft and numerous news reports of the theft or loss of laptops containing reams of sensitive government and personal consumer data.

Investigation into the use of biometric devices as an added layer of security has grown exponentially, and for good reason. A biometric identifier, such as a fingerprint, a person's voice, iris or retinal pattern is something everyone carries with them. There is no cost to provide it and there is nothing to lose. This paper focuses on one such biometric application; voice authentication, as an easy and cost effective way of enhancing security of consumer and enterprise applications. It discusses what voice authentication is, what its uses are, vertical markets that are embracing its use, and business drivers for using it as part of an enhanced multi-factor authentication enterprise strategy across channels of communication.

Voice Authentication Defined

Voice authentication, also called voice or speaker verification is one possible factor in authenticating that a person is who they say they are, for the purpose of providing secure access control. Typically when the industry and government regulators speak of authenticating a user for the purposes of security that authentication consists of three things:

- Something you have (key, smart card, credit card, badge, token)
- Something you know (social security number, mother's maiden name, account number)
- Something you are (biometric such as a voice or fingerprint).

Security applications can be set up with more than one factor. Two-factor authentication can be as simple as asking the person for more than one piece of information, such as account number and mother's maiden name, or a more complex combination of 'what you know' plus 'what you have'. The most common example of this is a person using an ATM card and PIN at an ATM machine. Two-factor authentication is also sometimes referred to as strong authentication. The use of three or more authentication factors is referred to as strong authentication or multi-factor authentication.

Voice authentication, as with other biometrics, is based on an individual's unique physical characteristics; in this case the physiology of the person's vocal tract, along with specific behavioral ways of speaking. A person being enrolled as a new user to a voice authentication system is asked to speak a word or phrase, and that utterance is captured and digitized as a "voice print", and then stored as a voice template in a database. The voice print/template is not a digital recording or an audio file, so it can't be impersonated by a recording. Voice prints can also be encrypted, and until they are mapped to account data, they are meaningless in identifying a person. When the voice authentication portion of an application is used the person is asked to speak a

required password or phrase and the system compares that utterance with the stored template, accepts or rejects the input, and then grants or denies access.

A voice verification application is very flexible in that it can be set up to request that the user utter a single word, phrase or password, or request that a random sentence or phrase be used. For applications that require more stringent security procedures, verification can be used in combination with a set of challenge questions (what you know), raising the threshold of which users will be accepted, or the system can be set up with less stringent authentication requirements for parts of an application (checking a bank balance, for example) and more for other parts (transferring money). Verification is ideally suited for the most stringent of multi-factor authentication applications. For example, the system can be set up to call out to a specified customer number, and ask the person a random set of questions, thereby combining 'what they have' (phone number), 'what they know' (answers), and 'what they are' (voiceprint).

Voice Authentication vs. Voice Identification

For the purposes of this paper we are talking about voice verification or authentication, not voice identification. There is a difference. With voice authentication the user has a voice template stored in a database that is definitively linked with their ID; perhaps their account number or social security number. When the user accesses the system that template is pulled up from the database as a result of that ID being supplied by the user, through caller ID, physically using a card, or entering a password, for example. The system then authenticates their utterance against that voice template. In essence, the user is making a claim about who they are, and the system is verifying that claim.

With voice identification, the templates are stored in the system, the user accesses the system and speaks, without supplying any other identifying information and the system must search through the database for the correct template, and then authenticate the user. The later is much more difficult for the system to do because the system is given one sample and is forced to search through the entire database, and come back with a best guess. Depending upon the size of the database, this can significantly affect confidence scores in matching. With authentication, the system is given the information as to which template to compare against.

Voice Authentication—Why Now?

So why consider using voice authentication? The reason is that it has never been truer that “the world has gotten smaller”. In the past three decades we have moved from a fairly homogenous population that both acquired goods and services and worked fairly close to home, to a very mobile population that works wherever they want, and purchases goods and services locally as well as over the phone and on the Internet. A vast amount of technology advances, including the introduction of the Internet, laptops, and mobile devices, has given companies more options in providing goods and services, pushing companies to incorporate more ways to service those customers. Now it seems more the norm for an enterprise to have a contact center and a web site for customer service than not.

The contact center in particular is the hub of customer service providing everything from retail orders to customer support. Contact centers are frequently the first window into a business, often replacing the face-to-face contact businesses used to enjoy. Unfortunately, with the rise of rewards that enterprises have gained through the use of contact centers, has come the rise of risks associated with providing services to customers through them. When we lessened that face-to-face contact we opened the door to a rise in fraud.

The “why” of authentication is that a fraudster can't talk their way around a voice print as they can with an agent, making authentication the perfect foil in a multi-prong security attack against fraud. Additionally, voice authentication has the advantages of:

- Being accessible remotely, over the phone or web, providing access to databases no matter where they are on the network.
- Being a natural user interface because it mimics what we do—speak.
- Taking advantage of existing technology investments such as interactive voice response (IVR) and computer telephony integration (CTI).
- Being easy to integrate into existing applications either as an on-premise application or hosted.
- Being the perfect component of multi-factor authentication, providing 'something you know' with 'something you are'.

In addition, following are other factors that have helped fuel the rise in the adoption of voice authentication in security applications.

Identity Theft

With the rise of the convenience of making financial transactions and buying goods and services through IVR, contact center agents and web applications, has been the meteoritic rise in fraud and identity theft. Fraudsters have tried all means of appropriating personal information from stealing mail, dumpster diving, or double swiping credit cards with a card reader, to stealing cards and PINs at ATMs. As identity theft has risen, it's only natural that fraudsters would turn to the telephone as a way to get sensitive information and make transactions. "Phishing" is the act of calling up a business and pretending to be someone you aren't; essentially fishing for information in order to get past the customer support rep or agent. For example, fraudsters often have just enough information, maybe one piece of a multi-question authentication process that they can use to sincerely feign ignorance and scam the agent into thinking they are someone they aren't.

Voice authentication has no sympathy for ignorance, and is thus one critical option in helping stem the use of stolen personal information to make fraudulent transactions.

Government Regulations and Guidelines

In response to issues such as identity theft and the loss of personal information, the government has implemented strict guidelines in how personal information should be accessed and stored. Although every industry is affected here are two examples of such government action in the fields of healthcare and finance.

In 1996 the government enacted the Health Insurance Portability and Accountability Act (HIPAA) which governs how consumers' personal health information should be gathered, transferred, accessed and stored. HIPAA stipulates that each consumer have a unique user ID, and that access to information requires dual-factor authentication, of which voice authentication is one option.

Within the financial industry, the Federal Financial Institutions Examination Council's (FFIEC) guidelines state

that using the commonly deployed username and password is insecure, and they encourage financial institutions to rethink providing multiple levels of security, either in a multi-factor identification or multi-layer security. The later, for example, might require that when someone calls into a financial institution to change an address that notification of the change is sent by mail to both the old and the new address.

Enterprise Data Security

It isn't just identity theft and the corresponding government regulations that is stimulating importance of security in the minds of IT professionals. The incidence of hacking, denial of service attacks, and viruses, are just a few of the growing and ongoing threats to network and database security. These threats have been the stimulus for myriad corporate rules and guidelines for employees to help protect corporate data, the least of which are rules governing the use of passwords.

With added security are added costs, including the amount of time IT spends on resetting employee passwords. Depending upon the industry, password reset can account for 10-60% of IT calls at a cost of \$10-\$45 per call. Automated password reset using voice authentication saves IT departments thousands of dollars per year.

Cost Savings and Simplicity

Voice authentication is simple to deploy and simple to use. Creating a user account and voice print takes a matter of minutes. Compared to some of voice authentication's biometric brethren, maintenance is a breeze as there is no retinal scanner or fingerprint reader to maintain, for example. Compared to alternative forms of security, such as an ATM machine, or RSA token implementations not only is voice authentication cheaper to maintain, its cheaper to deploy, without the added cost of replacing missing lost tokens, etc.

Customer Convenience

Without anything to carry, such as a card or key, voice authentication provides the utmost in customer convenience in that once the print is made; nothing more needs to be done. Unless multiple authentication factors are required, the voiceprint is the customer's key. Since the demand for better and more comprehensive customer support has risen

at the same time as security concerns have, providing access that is both secure, yet convenient is more important than ever.

Brand Image

With all of these other factors taken into account, when properly deployed with a focus on educating users as to what voice authentication is and the benefits of its use, the use of voice authentication can increase an enterprise's brand image because of the extra security it provides.

Take for example, the use of voice authentication as a way to provide physical security in a retirement community. A system can be installed using the phone system and speaker units at each front door, and other places around the community, with voice authentication via the speaker units, in lieu of keys. Not only does this eliminate the cost of periodic rekeying of the entire premises, there are no keys for people to use or misplace. The bump in image comes when residents not only don't have to keep track of their own keys, but they can set who else is allowed access to the unit, via voice, by time of day or week. For example, a cleaning person might have access one day a week, but no other time, not only providing security, but also not requiring that person to have a key.

Vertical Market Applications

The above market drivers have moved a number of industries to adopt voice authentication as part of a multi-factor authentication strategy. Among the faster segments to adopt voice authentication are:

Customer Service

As mentioned above, there are strong benefits for contact centers that implement voice authentication technology as a front end to a call. In a help desk environment voice authentication helps defray the cost of password resets by enabling users to reset their own. But even more basic than that is the cost savings a voice authentication application provides by handling the tedious and sometimes time consuming task of verifying who the caller is. If even a portion of each call is taken care of, that equates to a lot of savings over a year.

Financial services

The quickest to adopt voice authentication as a part of a security strategy has been the financial services sector. An early adopter of multi-channel customer support strategies, financial services companies have been among the first to broadly provide over-the-phone and web-based customer support. That strategy, combined with the criticality of the services they provide, along with government regulations and guidelines, have made financial institutions particularly mindful of providing tight security, without making it inconvenient or frustrating for the customers they serve. Voice authentication has provided them with an additional non-invasive way of protecting customers' data and money, in applications ranging from account balance and transfer, change of address, to portfolio management.

In addition, a small niche within the financial services industry that is a highlight of the effective use of voice verification is the utilization of a "voice signature" for what the industry terms the "underserved" community. The underserved aren't high wealth banking clients, but rather those people less likely to have checking and savings accounts, such as migrant workers, people traveling away from their home country, etc. The use of voice signatures allows a financial institution to provide on-demand banking services, such as money transactions, pre-paid purchases, and automated escrow payments from auctions sites, etc., to consumers without requiring minimum account balances.

For example, billions of dollars each year are transferred from one country to another by immigrants working in one country and sending money back to families in their home country. With voice signatures, a worker can set up to have their pay check automatically deposited into an account, call into the account, use their voice as their signature, and have money transferred back to an account in another country, without having to carry a check book, or use a wire transfer service.

Insurance

As with other vertical markets, voice authentication provides an added level of security for insurance subscribers, plus it provides additional benefits to insurance companies even before subscribers sign up. For example, when a new

subscriber is being signed up by a broker, there is typically a multi day time lag between the time a customer says yes, and the time they get the paperwork, sign it and return it. By using their voice print as their signature, new subscribers can be legally signed up that day and have coverage commence automatically with paperwork to follow.

Telecommunications

Telecommunications, particularly in the mobile space provides practical applications for the use of voice authentication in customer support situations. Voice authentication allows users to gain hands-free access to their accounts, without keying in passwords, when they want to manage their accounts. For example, a user can call and replenish minutes on a pre-paid card using their voice as their password.

Healthcare

Since the passing of HIPPA, many areas in the healthcare industry have sought to use voice authentication as an added layer of security, particularly when customers are accessing sensitive data, such as lab results over the phone, or creating a “transaction” such as refilling a prescription. Using voice authentication customer’s privacy is guaranteed and fraud is reduced.

From the healthcare provider side, voice authentication can be used for time and tracking of visiting healthcare workers, such as rehabilitations specialists or nurses, by having them call into the system from each patient’s home. The system can then track them by Caller ID of the home they are at, combined with their voice for authentication.

Government

Government applications for voice authentication range from solutions for internal employees (government workers) within vertical applications within government agencies, such as insurance, banking, etc., to horizontal applications such as time tracking and accessing personal information.

There are multiple voice authentication solutions for consumers related to government as well. Two examples, in particular, stand out for providing security to citizens. First, welfare agencies have used voice authentication solutions for determining that the caller is who they are to prevent both

fraud and to protect ex-spouses from getting information about their former spouse, as they are denied access to the system.

Another application offers both security and cost reduction. Voice authentication has provided the perfect solution for tracking parolees, those on house arrest, or sex offenders by making it so that they are required to be where they say they will be when they call in. The system calls at standard or random times and the parolee has to be there to accept the call, or they are asked to make a call and have their voice authenticated. This provides security as the system can’t be duped by a recording. Additionally, there is also significant cost reduction potential by not requiring that ankle monitors or other equipment be used.

Barriers to Entry

Perhaps the biggest barrier to entry for the deployment of voice authentication has been unawareness on the part of the consumer as to what voice authentication is, and lack of awareness campaigns by enterprises to help educate employees and customers on the benefits of its use.

A year after 9/11 we did a study on consumer’s awareness and acceptance of biometrics as a whole. The BioMarket Project, Public Awareness Pilot Study, a joint effort between Jamison Consulting and Brand Marketing Ltd., surveyed the public at large as to whether or not they were aware of what biometrics are and how they felt about their use. We included five biometric types in the survey including speaker/voice verification, fingerprint recognition, face recognition, iris scans, and handprint geometry. The survey included 25 in-depth qualitative surveys, and 200 over-the-phone quantitative surveys.

Although the study was done seven years ago, it was done at a critical period in time for the emergence of the use of biometrics. Not a lot of people were aware of the kinds of biometrics, the security provided, or the options for their use. Recognition rates for all biometrics were about 30%, with voice verification scoring the highest with 84% of those surveyed saying that they recognized the term. Although it also had the highest incidence of people thinking that the system could be fooled, verification prompted the most people to say that they would be willing to use it (84%).

Even though in general many respondents recognized what biometrics was as a whole, few had an in-depth understanding as to how the technologies work. As a result there was a lot of commentary on different fears that people had as to their use, which included the following:

Misunderstanding about how it works

Misunderstanding about how the various technologies work led to two distinct fears; that it would physically hurt them, and that their “persona” would be stored somewhere. For example, some were worried that a retinal scan could hurt the eyes. One person feared that it would burn their eyes like a laser. Others didn’t understand what was being stored and that it could be misused. Such responses showed that there was a lack of education as to how biometrics works.

Invasion of privacy

In the study, numerous people mentioned that they felt like capturing a “part of their body”, or even a representation of such was an invasion of privacy. This misperception of how the technology works point back to lack of education in that with biometrics, and in this case voice biometrics, the customer isn’t divulging any privileged information about themselves, particularly if the application asks for a random string of words to be spoken. And since everything is digitized and stored, the voice print doesn’t mean anything until its mapped to other information such as an account number, both of which can be encrypted anyway.

Big Brother

Those that were concerned about invasion of privacy also mentioned government interference in their lives as well. This quote is representative of the theme that once we employ biometrics we are headed down the path of “Big Brother”: “Just because there are a couple thousand terrorists in the world, I am not willing to start down the “slippery slope” to “1984”. Once you start with this where do you stop, where does it lead ten, twenty years from now?”

Who owns the print?

There was also concerned as to who owned the print. Do they get stored at the business that is using them? Can they be hacked? Not knowing left many people uneasy.

Cost

Finally, there was the issue of cost. People were concerned about the added cost of using biometrics everywhere. This fear was from citizens in general, who were concerned that cost would be passed onto them, and from business owners who were concerned about the added cost of providing a biometric security solution.

Deflecting Concerns

The good news is that in general, acceptance of biometrics was fairly high, and with some explanation as to how the various technologies work, it went even higher. When we got to the general questions on biometric use 69% of respondents thought that government and enterprises should be encouraged to use biometrics, even though their concerns about privacy were still there.

The change in perception once a technology was explained got interesting when we asked questions about where biometrics should be used. Here it became apparent that with education about the biometric, people’s opinion could change very quickly. For example, when we asked if biometrics should be used in hospitals, many people said no, until the question was refined to ask “How about in the nursery so that no unauthorized person could remove a baby”. Instantly the willingness to use it went way up. Across different scenarios it became apparent that if vendors would do a better job of educating consumers as to biometric use and benefits, acceptance would soar.

Similarly, when we explained the benefits of using voice authentication in finance 58% of the quantitative respondents saying yes, and 74% of the qualitative respondents, due to the convenience of not having to remember passwords, reset them, change them, or carry something with them.

Summary

Voice authentication is a practical, safe and secure way to enhance a multi-factor authentication strategy. Easy to deploy and easy to use, it provides a very convenient way for customers to access accounts or physical assets while reducing costs to the businesses using it.

Since barriers to the use of voice authentication in general center on misperceptions as to how the technology works, good pre-implementation marketing campaigns go along way in increasing the adoption of its use. Those business concerns, such as cost to implement the technology, can be quickly dismissed through business cases that show return on investment, such as in the case of password reset, or by providing voice authentication as a hosted option.

Lastly, a lot has happened in the time since that one study was done. People accept and are used to using speech recognition. Consumers are more used to enhanced security procedures and for the most part are more grateful for their use than annoyed by any minor inconvenience. With voice authentication, you can provide enhanced security with minimal inconvenience in a cost effective manner. What could be better?

About Convergys

Convergys Corporation (NYSE: CVG) is a global leader in relationship management. We provide solutions that drive more value from the relationships our clients have with their customers and employees. Convergys turns these everyday interactions into a source of profit and strategic advantage for our clients. For more information, visit www.convergys.com.

Corporate Headquarters

North America

Cincinnati, Ohio USA
Phone +1 513 458 1300
US Toll-Free 800 344 3000
Fax +1 513 421 8624
www.convergys.com

Regional Headquarters

Europe, Middle East, & Africa

Cambridge UK
Phone +44 1223 705000
Fax +44 1223 705001

Latin America

São Paulo Brazil
Phone +55 11 5504 6800
Fax +55 11 5504 6730

Asia Pacific

Singapore
Phone +65 6557 2277
Fax +65 6557 2727

relationship management