
Your voice is one in seven billion.

By DEBBIE PEACE, AAP, and Co-author, PETER SOULIERIS

With your voiceprint – a set of measurable characteristics of a human voice that uniquely identifies an individual– you can unlock everything from your smartphone to the U.S.-Canadian border through the US PORTPASS program. With this new functionality, however, some fear that it can also unlock the potential for increased fraudulent activity – activity that exists outside of current fraud avoidance technology and regulation. While mitigating fraud is challenging within any delivery channel, the perceived risks associated with voice biometric authentication are quite frequently more myth than fact.

The biometrics market as a whole has grown substantially in recent years due in part to accuracy improvements in the algorithms used to support voice biometric authentication as well as the increasing levels of adoption among verticals including mobile banking and financial services. Banks and credit unions have tapped into biometric authentication as part of a layered security measure to help combat rising risk concerns, and it looks as though many more are expected to move in that direction with a recent analysis by Goode Intelligence predicting that 1.9 billion bank customers will regularly use biometric interfaces by 2020.

Furthermore, within the next five years, the total biometrics market size is expected to surpass $50 billion, according to a new research report by Global Market Insights, Inc. This represents a significant leap from the $7 billion spent globally in 2014. Interest is growing. Regulators have been predicting the use of biometrics and encouraging adoption among financial institutions for nearly a decade, and in many consumers’ lives, biometrics as a layered security measure is already mainstream. Your iPhone is most likely unlocked by either a fingerprint or facial recognition to confirm identity. Google Assistant uses voice biometrics to unlock Android devices. Disney World has biometric authentication at turnstiles and in use throughout its parks. Once relegated to the realm of action movies and science fiction, biometrics has now become ubiquitous in daily life.

From enhanced security functionality to seamless authentication experiences, biometrics, and voice biometrics in particular, is changing the way customers interact with businesses and conduct everyday tasks. Despite the growing momentum and regulatory incentive, however, there still exists doubt surrounding voice biometrics as a secure, efficient and easy means of authentication.
Voice Biometrics as Fraud Fighter

Within the last five to 10 years, a customer needed to be present to visually confirm their identity and authenticate a transaction. Now, as consumers move rapidly to a digital marketplace to conduct their business, transactions take place in an increasingly “customer-not-present” environment. Voice biometrics has emerged as the closest (and easiest) interaction between two parties that are communicating remotely. Additionally, implementation of voice as a means of layered authentication is now cost effective and widely available, worldwide.

As a result, it has become more important to decode the biology, technology and myths behind voice biometric authentication as fraudsters become more sophisticated. According to Javelin Research, 2017 saw record high levels of identity fraud, with 16.7 million victims. Banks, credit unions, credit card companies and payment providers are among the most targeted as consumers move quickly to a cashless economy powered by e-payments and digital wallets. The recent breaches suffered by big brands once again highlight the importance of security in the digital economy and how users need to adopt the right procedures to try to protect their data. Consumers, businesses and financial institutions need a sophisticated means to verify legitimacy and combat the rising security risks.

In 2012, mobile banking set a new gold standard for customer convenience. Developments in voice technology are eclipsing those standards, and it is expected to have an important impact on how customers manage their money in the future. To reiterate this point, consider this: Most day-to-day banking tasks are the reason behind 85 percent of all web traffic to banking sites. The most common among these tasks is a basic balance check, requiring less than three minutes and as few as two page views per session. Voice technology and authentication can change that, and it is predicted that web traffic to online banking portals and for mobile applications will drop by nearly 50 percent in the next five to 10 years.

Voice recognition and authentication maturity are tipping the scales as banks and credit unions move to offering common banking tasks such as a simple balance check by talking to an Internet-enabled voice assistant. Voice biometrics will help create the frictionless, secure environment to make this move successful.

Every voice has a unique signature, a distinctive identifier based on personal biology. Voice biometrics can validate the identity of the user or caller by detecting more than 100 physical and behavioral factors in an individual’s voice patterns. This includes pronunciation, emphasis, speed of speech, accent, as well as physical characteristics of the vocal tract, mouth and nasal passages. The human voice has several identifiers that make it just as unique as a fingerprint.
Three Tips to use Voice Biometrics to Combat Fraud

1. One-time Interactive Voice Response (IVR) authentication
Call center fraud is typically higher than in other customer service channels. Voice biometrics can dramatically improve the customer experience by ensuring that authentication is simple and frictionless; reduce call center costs by keeping callers in the IVR; and reducing fraud losses by making it more difficult for a fraudster to compromise an account.

When a customer dials into the system, he or she will be asked to speak a common passphrase. Once authenticated, the customer may proceed with the transaction, limiting the need for customer/agent interaction. One of the main reasons this method is so successful is because it eliminates the poor authentication methods, from both a security perspective and user experience perspective, previously used. PIN numbers are easily corrupted and easily forgotten.

2. Call center oriented: Agent + Caller
In this passive/conversational approach, an agent can take a recording of an individual’s voiceprint to reduce the consumer’s level of involvement in the future. This can both reduce friction and enhance fraud detection capabilities. Large banks like Citibank are already using voice biometrics to automatically identify a customer while he or she speaks to a call center representative. It takes less than one minute for a customer to set up a voiceprint, which can then be utilized each time contact is made afterwards.

3. Create a voiceprint of the fraudster
Organizations can build both a positive AND negative voiceprint database. With voice biometrics, if a bad actor manages to perform a fraudulent transaction, then their voice is recorded, cataloged and flagged for future reference.

Fraud in the Voice Channel

There are different ways a criminal can use voice technology to commit fraud. The rise of artificial intelligence (AI), internet-enabled voice assistants and other voice-driven technology has been life changing for consumers, and game changing for fraudsters. Because of this, the likelihood of voice fraud is now on the rise. Most often, there are three basic avenues fraudsters take to gain access to personal or financial information: 1) something the user knows such as a password or mother’s maiden name; 2) something the user has, such as an ATM card, key, fob, or a token, and; 3) something the user is, such as biometrics identifiers.

With new technology, and new avenues, comes new opportunity for fraudulent activity. However, voice biometrics has proven beneficial in combating various types of fraud. Some of the most common fraudulent activities that can be negated with voice biometrics include:

1. Caller ID Spoofing
When a caller intentionally fabricates the information transmitted to a caller ID display to disguise their identity.
Oftentimes, this is used as a means or part of an attack against someone to trick them into providing valuable and personal information so that it can be used in fraudulent activity or sold illegally.

2. Vishing
A form of criminal phone fraud that uses social engineering. Fraudsters use deliberate manipulation that convinces people to divulge confidential information so that the fraudster may gain access to personal financial information. A vishing call can use a human or an algorithm-driven computer to actually interact with you, seeking out information.

3. Cramming
Fraudsters call their victims and ask a seemingly innocent question: “Can you hear me?” The answer “Yes” is all they need. Replaying a recorded affirmative response lets them subscribe their victims to paid services, which will be included in the victims’ phone bill.

As consumers increasingly turn to digital channels for account services, most often the call center bears the burden of mitigating this risk. Often, when consumers reach out to the call center, the first step in authentication is utilizing the “something you know” security measure. But many are not able to remember their banking passcodes or answers to predetermined security challenge questions.

With each call, traditionally, an agent must verify the caller’s identity through a series of knowledge-based authentication questions. It is at this juncture -- this particular point of weakness -- that fraudsters most often attack. Not only is this a vulnerable moment for an organization, but it is a frustrating one for its consumer as well. Instances like these drive up average call times and increase operational costs while driving down the overall customer experience. Meanwhile, losses tied to fraud originating in the contact center continue to climb.

Instead of using something you know (like a password), something you have (like a key), voice biometrics uses who you are to identify you. All biometrics use physical characteristics in some way. Unlike keys and passwords, your personal traits are extremely difficult to lose, forget, or forge. For this reason, biometrics is considered to be safer and more secure than knowledge-based or tech-based fraud prevention techniques.
Debunking Voice Biometric Myths

**Myth:** My password can be stolen if it is overheard in a public place.

**Debunked:** Contrary to popular belief, even if you say your password out loud, it can’t be stolen because your voice is your password, not the words themselves.

Your voice is what matters, to the degree where even if everyone in the world used the same password, it would still be unique.

**Myth:** Voice replication by fraudsters could be easily accomplished via high quality recording.

**Debunked:** This is highly unlikely as today’s audio recording devices lack the quality to trick the bi-identifiers.

Furthermore, it requires the hacker to create a decidedly advanced and sophisticated program that could use a person’s voice to repeat random phrases asked by the biometrics security system in place. The voice replication generated would sound unnatural and would trigger additional security protocols to protect the customer.

**Myth:** Voice biometrics fraud is growing exponentially due to call center vulnerabilities.

**Debunked:** Fraud as a whole is climbing — but this broad category includes identity theft from knowledge-based and tech-based activities, not voice biometric authentication — which is the most secure method available.

An individual’s voiceprint is even more secure than a fingerprint — making it a better solution for banks and credit unions.

As voice security expands, organizations need to develop strong, frictionless, multi-factor authentication for all channels that a consumer engages in. In the emerging conversational economy, banks and credit unions are reimagining voice activated consumer experiences. Multi-factor authentication using voice biometrics is the necessary next step for creating new opportunities, but this cannot, however, come at the cost of the customer experience.

Customer-Driven Security

Before they can access their accounts, customers often need to provide passcodes, personal identifiers and answers to several rounds of security questions. And to speak to a customer support agent they endure a similar process. Yet, within today’s marketplace, consumers increasingly demand frictionless authentication across all of the channels in which they engage.

“Frictionless” is the key. The more (needed) security added, there is an adverse effect on the customer’s experience with the transaction and with the organization. This can lead to decreased loyalty and levels of adoption. The user experience becomes a challenging one for financial services clients when asked to add a token to a password to a fingerprint to a voice authentication measure.

Striking a balance in a “customer-is-king” marketplace is the key to both appropriate security measures and customer experience. Voice biometrics has emerged as a means to providing frictionless authentication, and has gained attention for its potential to streamline the customer experience while preventing fraud. Enabled by the prevalence of web self-service and mobile applications, voice biometrics is widely used today to verify customers’ identities via digital channels.

One area voice biometrics are being used is in authenticating out-of-band verification of high risk transactions, such as wire transfers. Voice biometric authentication can be used by an IVR system waiting for a call from a consumer or business customer to verify a wire transfer originated in online banking, if the wire is over a pre-agreed upon dollar amount or going to a new beneficiary. While it is not uncommon for financial institutions to want recorded verification of all outgoing wire transfers, the process of notifying the customer of this need and
obtaining the recording, can be time consuming. With the use of an IVR and voice biometric authentication solution, financial institutions can automatically alert their customers of this responsibility and step required to get a wire processed, putting the task on the customer to complete, rather than the financial institution having to perform manual call backs.

New York’s Department of Financial Services (NYDFS) made history when it became the first state department in the nation to implement wide-ranging state cybersecurity regulations for banks. The regulations, known formally as the NYDFS Cybersecurity Requirements for Financial Services Companies, require thousands of financial institutions that do business in the state of New York to conduct a risk assessment and maintain a risk-based cybersecurity program.

One interesting aspect of the NYDFS Cybersecurity Requirements for Financial Services Companies is that they require affected entities to use biometrics as part of an MFA solution. As part of an MFA solution, biometrics are being used to verify high risk transactions after they come out of the online banking channel and before they are processed by the financial institution. In addition, voice biometrics are also being used not only to create a transaction but also behind the creation point and before the processing point. It’s just one example of how new regulations are spurring adoption of biometrics in a variety of industries.

The FFIEC has been suggesting it for years. The 2005 Guidance began the regulatory conversation before the technology was even truly matured. This original guidance was a major stimulus to the adoption of stronger authentication beyond standard username and passwords.

Updated in 2011, the “FFIEC: Authentication in an Internet Banking Environment” guidance recognizes the significant advances in criminal threats, both in sophistication and sheer frequency, reiterating its original directive to include authentication factors that are more difficult to compromise than single-factor methods. Biometric characteristics were included in the scope. The vision that this is where information security needs to go has been in place for more than a decade. The FFIEC has been encouraging the use of biometrics as new payment systems emerge and the industry demands anti-fraud measures for proper authentication of high-risk banking transactions.

Whether the industry takes note and follows in the footsteps of the US PORTPASS Program, The New York Department of Financial Services, or the FFIEC, voice biometrics as a reliable authentication and verification method cannot be understated – our online ecosystem depends on it.