Banking on biometrics.

Financial institutions are ditching passwords for biometric authentication – here's why.

Biometrics featured by CNN Money

CNN Money news story profiling leading banks' adoption of multi-modal biometric security solutions.

NUANCE

Table of contents

"We believe the password is dying."

Tom Shaw, vice president for enterprise financial crimes management at USAA, to The New York Times

PINs and passwords = a double fail

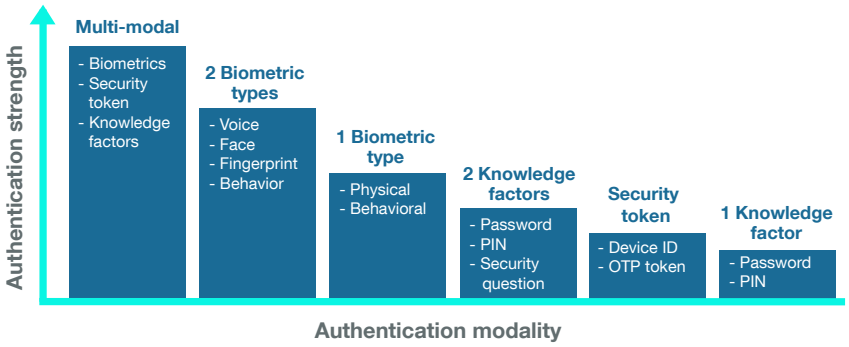
The financial services industry thrives on safety and security. Yet that's exactly what passwords, PINs, and other knowledge-based authentication factors are not. They're easily stolen and hacked, just as easily forgotten, and represent a true "double fail" to both customers and institutions: abysmal security and a terrible customer experience at the same time.

So what's replacing passwords? What steps are world-leading banks, brokerages, insurers, and even institutional investment firms taking to provide faster, friendlier access to customers while strengthening security?

Biometrics today – using more than one modality for secure authentication

The answer is biometric authentication. In this short primer, we'll show you how leading global financial services firms are embracing biometrics and the top technologies they're choosing. More importantly, we'll show you why these same firms aren't settling on a single biometric technology: they're using a combination of proven modalities to give more choice to customers while simultaneously achieving strong gains in efficiency and security.

For many, that makes biometric authentication a rare "no tradeoffs" solution. Let's look at why and how.



What is biometric authentication, who's using it, and why?

Simply put, biometric authentication is the practice of recognizing and verifying a person's identity through a unique physical or behavioral trait like the way a person talks, or the unique pattern of their fingerprint or eyes.

Once limited to science fiction and spy movies, today's biometric authentication technologies are highly sophisticated, secure, and increasingly commonplace. Today, hundreds of millions of consumers use biometric authentication every day, to unlock their smartphones and access their favorite mobile applications through built-in fingerprint scanners on their mobile devices.

It's not just device manufacturers that are embracing the technology. ABI Research projects that the global biometrics market will exceed $30 billion by 2021, with banking and personal finance companies leading the charge.[1]

According to the New York Times, many banks are already ahead of the curve:

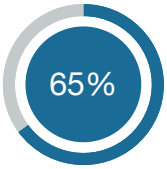
> Millions of customers at Bank of America, JPMorgan Chase and Wells Fargo routinely use fingerprints to log into their bank accounts through their mobile phones. Wells Fargo lets some customers scan their eyes with their mobile phones to log into corporate accounts and wire millions of dollars. Citigroup can help verify 800,000 of its credit card customers by their voices. USAA, which provides insurance and banking services to members of the military and their families, identifies some of its customers through their facial contours.[2]

It's a smart and timely move. According to research from Visa Europe, 75 percent of young adults (aged 16 to 24) are comfortable with the use of biometrics — even to make payments.[3] As a result, financial services providers are increasingly turning to biometric technologies as a "must-have" differentiator as they compete to earn the business and loyalty of young, upwardly mobile customers.

Barclays provides faster, easier access to account services
At Barclays, over 65 percent of calls are now handled by voice biometric authentication, providing enrolled customers much faster, easier access to account services. Instead of spending an average of two to seven minutes providing passwords, PINs, and answering security questions, Barclays' customers spend just 20 seconds verifying their identities with voice biometrics.

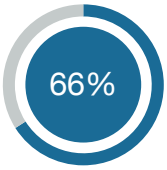
Banco Santander Mexico saves time and money
Banco Santander Mexico's adoption of voice biometrics reduced average authentication times by 42 seconds and achieved an annual savings of $1 million — ultimately winning a prestigious financial award for innovation in customer service.

Tatra Bank customers prefer biometrics
At Tatra Bank, voice biometrics cut authentication times by 66 percent — with 90 percent of customers reporting that they prefer voice biometrics to the previous system.



65 percent of Barclay's customer calls are now handled by voice biometric authentication.

Banco Santander Mexico adopted voice biometrics reducing average authentication times by 42 seconds, achieving an annual savings of $1 million.



66 percent reduction in authentication times when using voice biometrics at Tatra Bank.

1 http://www.biometricupdate.com/201603/new-report-predicts-global-biometrics-market-to-exceed-30b-by-2021
2 https://www.nytimes.com/2016/06/22/business/dealbook/goodbye-password-banks-opt-to-scan-fingers-and-faces-instead.html
3 "Young People 'Ready to Replace Passwords With Biometric Security," http://www.silicon.co.uk/e-innovation/biometric-security-replacing-password-visa-159680

Multiple modalities = more user choices, better security

As a category, biometric authentication technology is comprised of many different modalities (examples include fingerprint, iris, and voice). But according to Tiffany Huang, Research Associate at Lux Research, "(It's) hard to see one biometric usage winning in the medium- to far-term." More likely, according to Huang, companies will need to "consider multi-modal biometric platforms to stay in the game."[4]

A multi-modal approach is smart for many reasons, and one that many financial services providers are already pursuing. From a customer-experience standpoint, more modalities mean more choices. While voice authentication is great when a customer is calling from their home or office, it's less optimal on a crowded subway or a noisy city street. Similarly, fingerprint and iris scanners are great when you have a customer's captive attention, but may be less intuitive (and far more dangerous) if the user is driving home from work.

Secondly, taking a multi-modal approach enables powerful step-up security workflows. For example, a quick fingerprint scan in a mobile banking app might enable a customer to access their account balance or perform other low-level account management functions — but a request to transfer money, pay bills, or apply for a line of credit might trigger a request for iris or voice authentication.

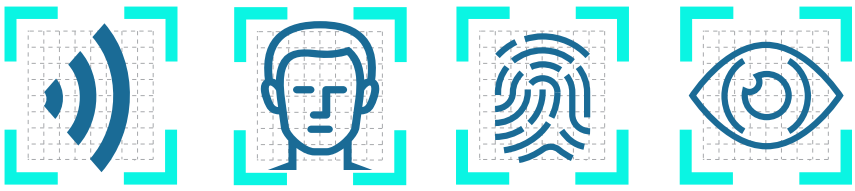
We'll explore the security benefits (and how biometric technologies can work together in a multi-modal approach) in more detail later.

Active and passive biometrics

Biometric technologies can be divided into two categories:

Active methods of biometric authentication

Analyzes physical characteristics (examples follow)



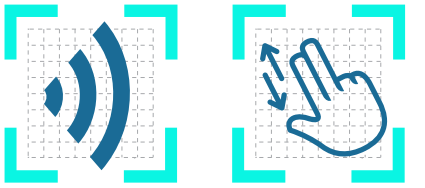
Voice biometrics | Facial recognition | Fingerprint scanning | Iris scanning

Active methods of biometric authentication require the customer to physically participate in the verification process by taking an action like speaking, placing a finger or eye in proximity to a scanner, etc. This method requires enrollment into the biometric system.

4 "State of the Market Report: Securing Mobile Payments with Biometric Authentication." Lux Research, March 31, 2016.

Passive methods of biometric authentication

Tracks these characteristics

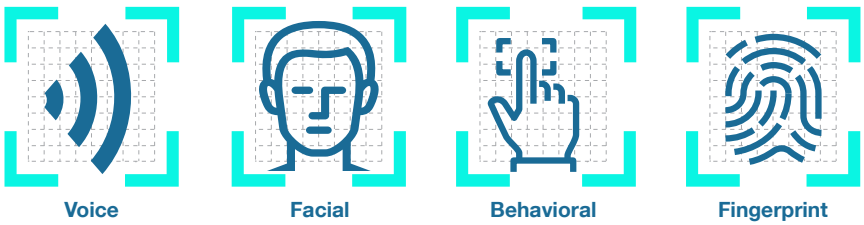


Voice biometrics **Behavioral biometrics**

Passive methods are capable of identifying a person without their active participation. For example, when a customer calls a bank instead of asking for account numbers or passwords, the agent merely asks "what can I do for you today." In the background the system "listens" to the customer and compares their voice to the voiceprint on file. Additionally a mobile banking application can quietly track user behavior like typing cadence, swiping patterns, and even geographic location to provide continuous authentication in case the user's session has been highjacked.

While new biometric modalities continue to emerge (from DNA and gait analysis to earlobe geometry and beyond), the technologies that are the most user-friendly and least intrusive are gaining the most traction across the financial services sector. Voice and fingerprint biometrics are highly prevalent in the financial sector due to widespread familiarity and ease of enrollment, while technologies like facial and behavioral recognition are also quickly gaining traction in mobile applications at some of the world's biggest consumer banking brands.

Smartphone biometrics – Ranking of security strength



Voice **Facial** **Behavioral** **Fingerprint**

Most secure to least secure

Most popular modalities for financial services

Here's a quick intro to each of the most popular modalities in the financial services sector:

1. **Voice biometrics**
   Voice biometrics allows customers to use their own voices in place of clunky passwords and PINs. According to a 2016 census by Opus Research, we're on track to hit a billion voice biometric enrollments — nearly 1/7th of the world's population — with at least 600 million of them in the next three years. With recent major releases by HSBC, US Bank, Royal Bank of Canada, and CitiGroup (among others), voice biometrics in banking is exploding.

Here's how it works: To enroll in an active biometric technology, a customer is recorded reciting a standard phrase like "My voice is my password," which is analyzed and turned into a "voiceprint." Then, each time they attempt to authenticate, audio is compared against the stored voiceprint — often while simultaneously being compared against a known fraudster voiceprint database for added security.

For financial services companies that want a more discrete enrollment process, passive voice biometric technologies are also readily available that enroll customers automatically using archives of previous calls. Then, customers are quietly authenticated during the first few seconds of every call, without being prompted for a passphrase.

Either way, it's fast, unobtrusive, and proven technology that is already in place at both major and regional institutions around the globe. Plus, it's far more secure. Unlike passwords (and other knowledge-based security methods which can be guessed or stolen), voice biometrics cannot be compromised in these ways.

Voiceprints are stored as a hashed string of numbers or characters, which have absolutely no value to a hacker since they cannot be reintroduced into the system in the same way as passwords. And each time a fraudster speaks with a voice biometrics-enabled IVR, call center, or mobile app, they leave behind their own voiceprint that can be used to proactively keep them out of the system and even alert law enforcement.

That means it's better for the consumer and for the corporation. On average, voice biometric authentication is 80 percent faster than knowledge-based authentication (like PINs and passwords), driving up to a $15 million average savings over a three-year period.

2. Facial recognition

Today's facial recognition systems are commonly used in security and surveillance in high-traffic public areas like border crossings, airports, train stations and stadiums. But financial services providers are also employing it successfully at ATMs, bank branches, and even bringing facial recognition technology straight to their mobile and Web applications and ecommerce security protocols.

During enrollment, these facial recognition solutions capture or analyze a submitted photo of the user, then perform a series of measurements (like eye socket depth and distance between the eyes, the width of the nose, etc.) Then, the system can compare live or prerecorded surveillance footage against its database of enrolled users to identify customers.

At HSBC, where almost half of all new accounts are opened online,[5] new business customers can now open a new account by taking a "selfie" to verify their identity.

MasterCard has taken a similar approach, announcing plans in 2016 to bring "selfie pay" security checks to more than a dozen countries.[6] If further authentication is needed during the checkout process for an online purchase, MasterCard will ask customers to hold their mobile devices up to their faces and blink, enabling fast and secure identify verification that does not impede commerce or inconvenience card holders the way declined or "more information needed" purchases often do.

5 "HSBC customers can open new bank accounts using a selfie," CNBC, Sep. 2016
6 "MasterCard unveils 'selfie' security checks, says heartbeat authentication could follow," The Verge, Feb. 2016.

3. Fingerprint scanning

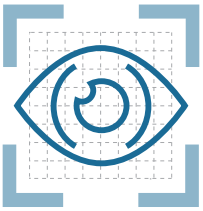
In 2016 alone, Chinese smartphone vendors were projected to ship 200 to 300 million fingerprint recognition-enabled smartphones. And analysts once predicted that almost a billion mobile devices would be equipped with fingerprint sensors by 2017 — a figure that now seems quaint in light of impressive sales figures from major manufacturers like Apple and Samsung.

In response, major institutions like Bank of America, BBVA Compass, Deutsche Bank, CapitalOne, Chase, Lloyds Bank, and more now offer fingerprint sign-in to consumers on Android and iOS-based banking applications. And since customers are already accustomed to using their fingerprints to unlock their phones and make purchases in popular music and app stores, it's natural that they will feel more comfortable enrolling using fingerprint authentication in banking and other applications.

To date, the most progress in this space has centered on mobile devices — although fingerprint scanners are also becoming increasingly commonplace at bank branches. At First Bank, more than 850 full-and part-time employees use fingerprint scanners to log into workstations and access 76 different Web applications across the enterprise.

At bank branches and supermarkets across Poland, 2,000 ATM machines identify customers by the unique pattern of veins in their finger. Many Japanese banks use the same technology to monitor access to safety deposit boxes in branches.[7]

4. Iris scanning



Some mobile device manufacturers are embracing iris-scanning technology as the next generation of smartphone-integrated authentication. Microsoft and Samsung already offer built in iris scanners in devices available today, while Apple is expected to follow suit in 2018.

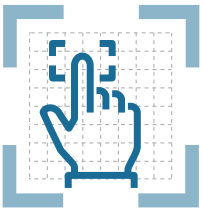
During enrollment, a camera (often integrated into a smartphone or tablet) digitally photographs a user's eyes using both regular and infrared light, capturing nearly 250 unique identifying features — about 5 times more than fingerprint systems typically capture.[8]

Earlier widespread deployments of iris-scanning technology were typically found in airports for security screening against "watch lists" — and today, several hundred million people are enrolled in iris-scanning programs for expedited travel programs including passport-free border crossings.[9]

Diebold and Citibank recently unveiled an iris scanner-equipped ATM that promises to dramatically increase the speed and security of cash withdrawals. The technology connects to the user's smartphone as they approach the ATM, giving them instant access to cash after authenticating through iris-scanning technology.[10]

7 "Forget fingerprints – banks are starting to use vein patterns for ATMs," The Guardian, May 2014.
8 "How Iris Scans Work" by Chris Woodford, July 2016, http://www.explainthatstuff.com/how-iris-scans-work.html
9 https://en.wikipedia.org/wiki/Iris_recognition
10 "The Eye Scanning ATM is Here," Oct. 25, 2015, The Wall Street Journal

5. **Behavioral**
   Most modern smartphones are also equipped with a wealth of sophisticated technology like accelerometers, gyroscopes, touch screens, and GPS. In behavioral authentication, a user is authenticated by the unique way in which he or she interacts with the phone — like how they type or swipe, or the angle at which they hold the device



   It's not just limited to smartphones and tablets, either. Top behavioral solutions can extract and analyze over 500 unique parameters (from mouse and track pad patterns to typing cadence and browser events) as they track how users interact with both Web and mobile applications — identifying fraudulent behavior and providing a risk score for each transaction.

   That means that even if a criminal can log in successfully using a stolen username and password, a bank using behavioral biometrics to analyze their keystrokes and other interactions with a PC or mobile device can still thwart them — ultimately determining that they are not, in fact, the authorized user they have logged in as.

   At National Westminster Bank in London they track and analyze virtually every move that customers make on both their Website and mobile application, looking for behavior that may flag that a user is not who they say they are.[11] And since behavioral technology is passive and doesn't require user enrollment, it's often used in tandem with other biometric security measures as an added level of protection.

Using biometrics for better experiences and better security

Each of these individual technologies represents a significant improvement in customer experience over PIN and password based authentication — and most provide substantial gains in efficiency and security, as well. They authenticate significantly faster and offer strong security advantages that PINs and passwords cannot.

First and foremost, biometric data is not stored in an identifiable way on either mobile devices or in the backend databases that provide authentication. Even if a hacker obtains the device or penetrates the database, the information (typically a cryptographic key) is almost impossible to retrieve or reassemble in a usable fashion.

Secondly, biometric data is extremely hard to fake. The most sophisticated technologies in use today include "liveness detection" features that can determine the difference between an actual person and pre-recorded or synthesized voice or an actual fingerprint versus a scanned rendition or modeled impression.

But the biggest potential returns come from giving customers authentication choices that cater to both their personal preferences and situational context, and using multiple biometric modalities in tandem to unlock powerful step-up and multi-factor security workflows.

11 "Next Gen Biometrics: Using the force of habit," November 2017, AmericanBanker.com

Customers want smarter choices

There's no question that customers have higher expectations now than they did a decade ago. But that's largely because advances in technology and savvy new business models now make it possible to turn historically poor experiences (like hailing a cab) into seamless, satisfying, and even share-worthy ones.

For the banking industry, authentication has been that historically poor experience. To fully remedy it, financial services providers can't simply replace passwords with a single biometric modality and call it quits. They need to provide smarter choices that fully empower customers to have a more effortless experience in nearly every circumstance.

For example, a customer may prefer using facial recognition from the comfort of their own home, but feel self-conscious posing for the camera to authenticate when they are at the mall or the office. Here, a combination of fingerprint and voice authentication would provide the customer with a fast and discrete mode of authenticating, while in turn reducing risk for the bank.

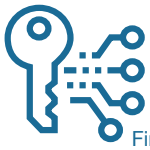
Similarly, it makes sense to use voice authentication to log in and check your bank account balance when you are somewhere quiet — but not at a music festival, where the background noise might drown out the customer's own voice.

By taking a multi-modal, platform-based approach to biometric authentication, financial firms can offer customers flexible choices that accommodate both preference and context.

More modalities = strengthened security

As early as 2014, one major global bank with over 70 million customers was piloting a multi-modal biometric security solution, incorporating both voice and facial recognition technology into their mobile banking app. By combining just a few spoken words with a camera snapshot, customers could quickly and easily access their accounts without fumbling with passwords and security questions.

Combining two or more biometric modalities improves security and confidence



- Voice biometrics
- Facial recognition
- Behavioral biometrics
- Fingerprint scanning

By combining two or more biometric modalities, a financial services company can benefit from both:

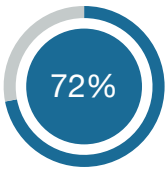
Multi-factor authentication, or using two or more different authentication factors to verify that a person is who they say they are.

Step-up authentication, where customers are prompted for stronger authentication methods as they attempt to access riskier, more sensitive resources.

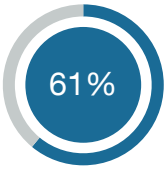
It's not hard to imagine the powerful and easy-to-implement scenarios that creative financial institutions will come up with. A mortgage servicer could allow customers to view account balances and make payments with a single fingerprint swipe — but require a facial and iris scan from each borrower before a home equity loan distribution can be made, for example.

And credit card issuers could use behavioral data to confirm that a customer is physically at the location where an account purchase is being attempted — then prompt the customer via their mobile application for additional biometric authentication as needed.

Brokerage firms may use similar workflows to identify unusual trading patterns, and to ensure that only the authorized (and verified) account holder is making buy and sell requests. In areas where fraud is rampant and the stakes are disproportionately high, customers will appreciate the added layers of protection.



72 percent of early Millennials feel secure with mobile fingerprint authentication.



Three in five people (61 percent) believe that biometric identification is just as secure or more secure than the current systems of passwords. (12)

Putting customers at ease

There's no question that biometrics is booming in banking and finance. It is improving CSAT and Net Promoter Scores, reducing risk, and improving key key operational measurements along the way.

But how do customers feel about it? Beyond the prospect of more convenience and choice, how comfortable is the average user with providing sensitive biometric data to the companies they do business with?

It turns out, acceptance is already widespread. In a recent survey from Experian, three in five people (61 percent) believed that biometric identification is just as secure or more secure than the current systems of passwords.[12] And 62 percent of US consumers feel secure with mobile fingerprint authentication, according to a 2016 consumer trends survey, with the number rising to 72% for early Millennials.[13]

The remaining resistance is likely to erode quickly as consumers grow more accustomed to the technology in their everyday lives. According to Juniper Research, more than 770 million biometric authentication applications will be downloaded each year by 2019 — up from just 6 million in 2015. And a report by Acuity Market Intelligence forecasts the biometric market will reach 2.5 billion users with nearly 4.8 billion biometric devices by 2020.

Your customers are on board. Are you?

Today, it's not a question of if banks and leading financial services firms will replace PINs and passwords with biometric authentication – it's when many have recognized the security risks and poor user experience inherent to knowledge-based authentication, and more are following suit every day — and most will follow suit.

The bigger question is which institutions will deploy the technology most effectively at scale, with the greatest returns — ultimately associating their brand with high value, low-effort services that today's customers have come to expect.

12 https://www.financedigest.com/the-rise-of-biometric-technology-in-banking.html
13 "The Smartphone is the New Bank," Nov. 2016, www.thefinancialbrand.com

To get ahead of that curve, we recommend:

– **Enlisting experts with a proven track record**
Since most financial companies do not have an in-house biometrics expert, you'll want to partner with an organization that has experience developing and deploying multiple modalities of biometric authentication technology. In biometrics, the right expert can add tremendous value — from the technical design of the solution to the go-to-market strategy (and even identifying the best use cases to lift utilization rates).

– **Planning for cross-channel from day one**
Even if your initial application for biometrics is limited to a single channel, we recommend planning for cross-channel implementation at the onset of the project. After all, once customers grow accustomed to using facial, voice, or fingerprint authentication in your mobile app, they'll expect them in your Web applications as well.

Having this vision early will ensure that the right technology is selected and the right infrastructure created to allow you to scale easily and affordably. More importantly, an omni-channel approach will ensure a consistent experience across all of your customer-facing interaction channels.

– **Offering more than one biometric modality**
Customers want choice, after all — and they also want easier experiences. With two or more modalities, the user can fall back on one if the other fails for any reason.

And since customers also expect consistency, we recommend ensuring at least one of your biometric modalities becomes a regular "staple" across all of your channels. Voice biometrics, for example, works equally well in mobile applications, the contact center, in branch locations, and across all your digital channels — giving customers a familiar experience no matter where they turn for service.

About Nuance biometric security

Nuance Enterprise is the global leader in biometric security, allowing consumers to choose how they authenticate while mitigating fraud at some of the world's leading financial services organizations. To learn more, please email us at customerexperienceexperts@nuance.com.

Resources to make the business case

Check out these additional resources to explore biometric security.

CASE STUDY

Adiós to PINs, passwords, and security questions.

Learn how millions of Santander customers simply use their voice to securely access their accounts.

Download Now

INFOGRAPHIC

Voice biometrics goes mainstream.

Decoding the biology, technology and myths behind voice authentication.

View Now

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

NUANCE

NUAN–CS–3112–01–FISERVE-WP, Mar 20 2017