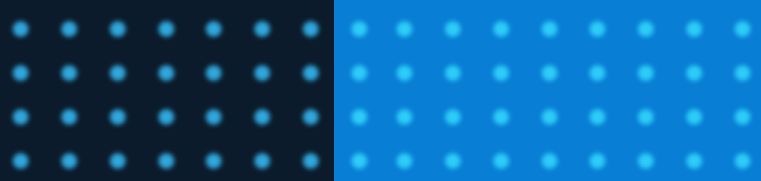


Beyond passwords: A guide to biometric authentication

Understand the state of biometrics today, and how to evaluate the right solution for giving trusted customers access to their accounts.





Passwords are a relic of the past

Passwords are a challenging and a highly imperfect solution for granting account access to your trusted customers. Asking customers to re-assert their identity at every touchpoint only leads to frustration and abandonment. And passwords leave customers vulnerable to identity theft and account takeover attacks.

For financial services firms and their customers alike, the risks and costs associated with passwords far outweigh the benefits.

Biometrics that can leverage widely available consumer devices are a more secure and convenient way to authenticate customers. But not all approaches are equal. In this e-book, we'll tell you why, and what to consider in your journey to a passwordless future with device-enabled biometric authentication.

WHAT'S INSIDE

- The problem with passwords
- Toward a passwordless future
- Biometrics as a replacement for passwords
- Evaluating approaches to device-enabled biometrics
- Additional considerations
- Common use cases in financial services

The problem with passwords

Passwords have been the foundation of digital access and identity authentication for decades. However, simple passwords – even when strengthened by additional factors like one-time passcodes – are no longer enough to defend against determined bad actors. Here are the main reasons why so many organizations are looking for alternatives to passwords:



VULNERABLE TO ATTACK

Passwords are notoriously easy for hackers to steal, intercept, or guess¹. Organizations can combat these vulnerabilities with additional factors including OTP and tokens, but these also have well-documented weaknesses that hackers can exploit.

Over 80% of the breaches to web applications can be attributed to stolen credentials.

2021 Data Breach Investigation Report, Verizon.



RISING COSTS

One of the top reasons customers contact a call center is for a password reset. Password resets and account lockouts take up an enormous amount of IT help desk and call center resources each year – time that could be better spent on more strategic projects. According to Forrester, the average labor cost to reset a single password is about \$70.

The average help desk labor cost for a single password reset is about \$70.

Forrester Research



POOR CUSTOMER EXPERIENCE

With more online accounts, people have more passwords to remember. Password-weary customers often choose weak passwords and reuse them for different accounts, making them even more vulnerable to attacks.

The average user has 100 passwords.

NordPass study, 2020

A close-up, vertical photograph of a woman with short, dark hair. She is looking down at a smartphone held in her hands, with a slight smile on her face. The background is dark with out-of-focus city lights, creating a bokeh effect. The lighting is soft, highlighting her features. A small, faint white square is visible in the upper left background. The overall mood is calm and focused.

“91% of organizations say that stopping credential-based attacks is the #1 priority for pursuing passwordless authentication.”

Reducing the reliance on passwords is obviously the first step to a passwordless future. Toward this end, many organizations are now looking closely at device-enabled biometric authentication. Instead of typing in a password, why not let customers gain access to their accounts with a selfie or a thumbprint?

“64% of customers trust biometrics over traditional passwords and knowledge-based questions.”

Biometrics as a replacement for passwords

To understand how biometrics can address the vulnerabilities of passwords, let's start by looking at authentication methods in practice.

Authentication is the process organizations use to prove the digital identity of the customer – is the person trying to access our systems really the trusted customer they claim to be? Current methods rely on one or more factors – something you know, something you have, or something you are. The more factors involved, the harder it is for attackers to gain access to your customers' accounts.

To protect against identity theft and comply with state and federal regulations for (SCA), many financial institutions have implemented two-factor authentication (2FA) or multi-factor

authentication (MFA) to confidently protect customer access to online accounts.

While 2FA and MFA are important steps toward better identity and access management, additional factors can add friction to the customer experience. And simply adding factors may not be sufficient. For example, knowledge-based questions and answers can easily be socially engineered, tokens can be compromised, push notifications are routinely accepted erroneously, and one-time passcodes delivered via SMS/text are easily thwarted with SIM card swaps.

Many organizations are looking at device-enabled biometric authentication as a more secure, convenient authentication factor than passwords only or passwords + 2FA.



Something you *know*

A password or answers to security questions.



Something you *have*

A mobile phone or a token.



Something you *are*

An inherent biometric characteristic such as your face, thumbprint, or voice.

Evaluating approaches to device-enabled biometric authentication

Giving customers an option to access accounts using biometrics on their devices instead of passwords typically involves one of two approaches, each with clear implications for convenience and security.

On-device biometric authentication

Apple, Google, Microsoft, and others have banded together with the FIDO Alliance to enable passwordless authentication on widely available consumer devices. Financial services organizations leveraging FIDO protocols enable customers to use their devices to sign into online accounts automatically, using on-device face detection or fingerprint recognition to verify their identity.

But what happens if face biometrics fail? The device typically defaults back to a passcode for access (often as simple as 4 digits) or prompts the user for login credentials and a password – which adds friction and is relatively easy to thwart. Like most credential-related attacks, the weakest link is the human. It's well known that people enroll the faces and fingerprints of friends and family on their devices, and the sensors on the devices themselves are not foolproof.²

For financial services organizations with stringent KYC requirements and low risk tolerances, on-device biometric authentication may not be sufficient – just because a person can unlock a device with their face or thumbprint doesn't prove they are the rightful owner of the account.



What is FIDO2?

The FIDO2 standard is intended to eliminate passwords using multi-factor cryptographic tokens.

FIDO2 leverages WebAuthn in the background, an open standard that enables strong public key cryptography to ensure user presence at the point of authentication.

FIDO2-enabled devices rely on unique digital keys that are easy to use and impregnable to theft – keys can't be shared and are stored on the customer's device. Users access their FIDO sign-in credentials by unlocking their device with their face or thumbprint.

Evaluating approaches to device-enabled biometric authentication

Giving customers an option to access accounts using biometrics on their devices instead of passwords typically involves one of two approaches, each with clear implications for convenience and security.

Cloud-based biometric authentication

Enterprises that want a more platform-agnostic solution deploy biometric authentication directly within their online customer experience or mobile app. In this case, biometrics enable an authentication factor separate from the device – a true second factor. Using any biometrics-enabled smartphone or computer, customers log into their accounts securely with their face or voice, which is matched to the verified biometrics template of record – no PIN or password required. And if the device is lost or stolen, no one who manages to unlock the device will gain access to that person's online accounts.

With this approach, organizations can quickly and securely use cloud-hosted, server-side biometric matching – with no reliance on the customer's unique device. Third-party solutions can provide organizations with more control over customer enrollment and configuration including the choice of biometric modalities – face, voice, or both to suit risk tolerances and business needs.



DEVICE INDEPENDENT

Accessible from any biometrics-enabled device



AI-POWERED

AI-trained algorithms ensure accurate and bias-free authentication



MULTI MODAL

Layer face, voice and liveness checks for added protection

Comparing biometric authentication approaches

	On-device biometric authentication	Cloud-based biometric authentication
User Experience	 Simple	 Simple
Biometric verification method	 Face ID, Touch ID, Windows Hello, etc.	 Face and voice including liveness detection embedded in UX
Authentication factor strength	 Single biometric signal	 Single, multi-modal, or dynamic biometric signals to suit use case
Approval thresholds	 Not customizable	 Fully customizable
Assurance levels	 Vary based on implementation	 High, with step-up verification layers as needed
Accuracy in blocking fraudsters	 Access to devices can be hacked or shared	 Biometric matching algorithms can evolve faster to keep pace with new threats
Device Independence	 Not yet	 Yes
Anti-bias	 Smartphone cameras have known weaknesses ³	 Algorithms trained and tested against balanced and representative data help eliminate bias in biometrics

Additional considerations

While it's possible to give customers access to their accounts with just a face scan or a thumbprint on their smartphone, enterprises are better protected by deploying biometrics as an authentication factor separate from the device.

What should you consider when evaluating biometrics as a replacement for passwords?

1 COST OF IMPLEMENTATION

Leveraging the devices your customers already own is the first step in reducing the cost of implementing biometric authentication. Look for solutions that can be deployed quickly in the cloud or natively within iOS and Android platforms, without requiring investments in new, dedicated servers or added costs of storing and administering biometric templates in compliance with international, federal, and state regulations including GDPR, CCPA, and BIPA.

2 MULTIPLE BIOMETRICS MODALITIES

Each use case will require different trade-offs between convenience and security. Consider whether the solution enables you to layer biometric modalities, add liveness detection for even stronger protection, or implement step-up measures when warranted. Layering biometrics modalities (face and voice combined) is 100 times more effective in deterring fraudsters than face or voice alone.⁴

3 ACCURACY

Biometric authentication accuracy is subject to two errors. Access granted to an unauthorized person is measured by the False Acceptance Rate (FAR), while authorized customers denied access is measured by the False Rejection Rate (FRR). Error rates can happen due to environmental factors (the conditions in which the face scan or voice print are captured) or when people age or even change genders. Look for solutions with sophisticated and continually updated matching algorithms to best ensure access for your good customers while blocking access for fraudsters.

4 STORAGE OF BIOMETRIC DATA

The choice between storing biometric data on the customer's device or on independent servers requires careful thought. Third-party solutions keep biometrics safely stored apart from the device and tied to the user rather than the device – delivering much stronger security without adding any additional friction. Users can change devices without having to re-enroll their biometrics. Look for solution providers who can keep your business compliant with data security best practices and complex regulatory requirements as they evolve.

Additional considerations cont.

5 DEFENSE AGAINST SYNTHETIC FRAUD AND BIAS

AI-based technologies specific to face and voice are more secure and sophisticated in defense against Account Takeover (ATO) attacks. Third-party solutions also provide the ability to check new users against a watchlist of repeat fraudsters, while consumer-grade biometrics do not. Look for solutions that enable active or passive liveness detection, can detect spoofs (masks, photos, or videos of faces), and have passed ISO 30107-3 independent lab testing for Presentation Attack Detection. Algorithms continually trained and tested against these scenarios, using large and representative data sets, are better able to deliver spoof-proof authentication and accurate results regardless of race, ethnicity, age, or gender.

6 CUSTOMER EXPERIENCE

Make sure your authentication flows capture the customer's biometrics in a seamless, secure, and hassle-free experience founded on trust and speed. Capturing biometrics accurately and quickly is critical to removing friction while increasing assurance levels and avoiding additional friction, either by adding a step-up layer to the experience, or worse, requiring the customer to contact your support team. Look for solutions that provide a seamless enrollment, authentication, and recovery journey for all user groups, device types, and software platforms.

Common use cases in financial services

See how financial services organizations are replacing passwords with enterprise-grade biometrics in a wide variety of use cases.

Offer a safer, simpler sign-on



Give trusted customers the option to enroll their biometrics as a safer, easier way to access their accounts.

How it works:

Upon login, Jessica is guided to take a selfie and/or record a phrase to enroll her biometric template. The next time Jessica logs in, she can do so with a selfie or voiceprint, which is quickly and securely matched against her template on file.

Advantages:

Passwords are a hassle for customers and susceptible to attack. Biometrics are unique to each individual and extremely difficult for fraudsters to fake.

Prevent ATO fraud



Capture and enroll a biometric template during onboarding to use throughout the customer lifecycle.

How it works:

During the initial onboarding process, Susan's identity is verified using a combination of ID document capture (is the document legitimate?) and live facial biometrics (is this the genuine owner of the document?). The biometric captured is stored securely as a template. When Susan accesses her account in the future, or applies for new offers, a new selfie or voiceprint is compared against the stored template. If it's a match, Susan is authenticated.

Advantages:

Biometrics stored independently of the device eliminate problems such as SIM card swaps that enable unauthorized users to gain access to accounts simply by unlocking the device.

Reduce call center traffic



Empower customers with secure self-service access for password resets or account changes.

How it works:

Jeff is a trusted bank customer with a biometric template on file. Recently divorced, he needs to remove his ex-wife from his accounts. What in the past would have required the help of a customer service agent can now be done quickly using a new selfie or voiceprint, matched against his template on file, to gain access and make changes to his account profile.

Advantages:

Biometrics provide a layer of protection that is much more effective than passwords in delivering assurance levels banks require for higher-risk customer activities.

Summary

Secure, frictionless biometric authentication for the enterprise

Financial services organizations are faced with the difficult task of strengthening security without compromising the overall user experience. Biometrics can offer a reliable way to authenticate customers without relying on passwords. It's important to evaluate solutions that not only can deliver a frictionless experience for good customers but also deliver the security, control, and flexibility financial services firms need.

Learn how Mitek can help

MiPass, with its state-of-the-art facial and voice biometric capabilities, provides increased protection against today's most sophisticated forms of identity theft and increasingly dangerous fraud techniques, such as deepfakes and synthetic identities. These technologies ensure the highest level of security against evolving threats while delivering a superior consumer experience.

Find out more at miteksystems.com

A NASDAQ® company | miteksystems.com Copyright © 2022 Mitek Systems, Inc. Confidential. All rights reserved.

This document is for general information purposes only and is not intended to be and should not be taken as legal and/or regulatory advice on any specific facts or circumstances. All information provided in this document is provided "as is" without warranty of any kind, whether express or implied. Contents contained in this document may not be quoted or referred to for any purpose without the prior written consent of Mitek or its affiliates.

