Prove

Multi-Factor Authentication (MFA) Buyer's Guide – How to Upgrade to True MFA

By Ken Palla, Bill Fish, Patrick Merfert, and Fitzwilliam Anderson

Table of Contents

Multi-Factor Authentication (MFA) Buyer's Guide – How to Upgrade to True MFA

Today, we're constantly bombarded by news about data breaches, credential stuffing attacks, and account takeover (ATO) attacks against banks, e-commerce companies, and cryptocurrency exchanges. The underlying weakness that fraudsters exploit in these cases is the use of passwords (weak or otherwise) and one-time passcodes (OTPs). Both traditional passwords and OTPs are the primary authenticators of choice that businesses are providing for millions of consumers in 2022. Keep reading to learn how we got here.

Note: *We want this Buyer's Guide to be as helpful as possible to you. We're going to start by defining what MFA is and providing an overview of existing MFA challenges, but if you're reading this, chances are that you're already familiar with these basics. If so, skip ahead to the* ***"Guidelines For Deploying MFA"*** *section.*

A Brief History of Modern Authentication

Between 2007 and 2011, companies first started to add Knowledge-Based Authentication (KBA) challenge questions and OTPs as step-up authentication methods in addition to just passwords. The main thing that many fraud and risk professionals might remember from this period is that consumers were quite confused. For example, when creating challenge questions for themselves, many consumers just added any random answer thinking that they would never actually have to answer the challenge question in the future. Soon, call centers were flooded by customers who were locked out of their accounts because they could not remember the answers to their own challenge questions. These overwhelmed call centers highlighted the importance of the customer experience as an integral component of consumer authentication and the need for better authentication methods.

Multi-Factor Authentication – The Challenges Companies Face Today

Fast-forward to today and customer experience is now an even more critical factor to consider given the increased volume in digital transactions *and* the increased competition between service providers to offer the most seamless experiences to busy consumers. Many companies are investing heavily in SMS OTPs, while others are leveraging biometrics and passive mobile authenticators.

In the past few years, we have seen significant developments, including:

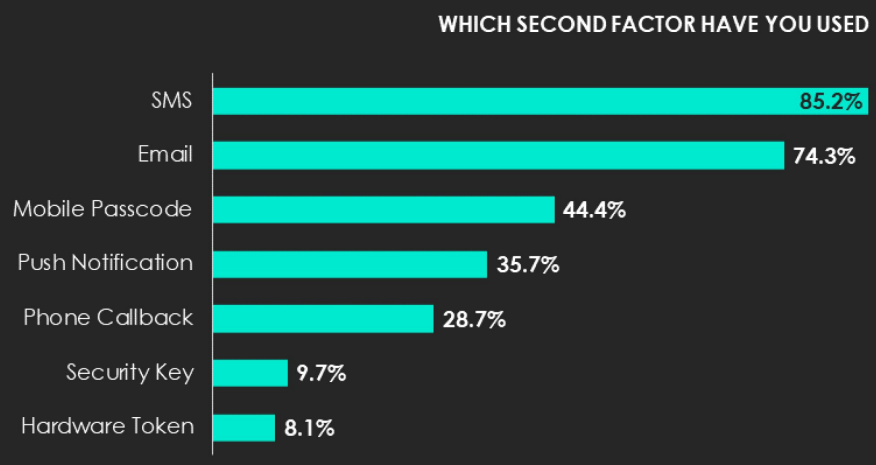
- The push toward passwordless authentication.
- The highly regarded FIDO2/WebAuthn standard for new authentication.
- The deployment of new biometric authenticators that give customers a choice of which biometric modality they would like to use.
- The deployment of Google and Microsoft authenticator apps.
- The migration of physical tokens – which have been the hallmark of sound commercial authentication for years – into soft token apps.
- The successful FIDO2/WebAuthn passwordless deployments in both the web and mobile environments with platform authenticators (Windows Hello) and roaming authenticators (e.g., Yubico keys).

Despite all of these developments, the vast majority of financial institutions, e-commerce companies, fintechs, and crypto exchanges still use SMS OTPs, Voice OTPs, or just passwords as their primary authenticators, which has led to major vulnerabilities and increased rates of fraud that are well-publicized in the news.

There is some good data to look at the state of MFA today. As illustrated by the graph below, consumers are growing more familiar with many different forms of two-factor authentication.

MFA Datapoint 1: Duo Labs surveyed consumers in the U.K. and U.S. about the use of authenticators[1]

[1]Duo Labs "State of the Auth 2021." Duo Labs surveyed 1,039 adults in the United States and United Kingdom.



Notice that 85.2% of consumers indicated that they have used SMS for 2FA, while 74.3% said they have used email as a second factor.

MFA Datapoint 2: In the business world, Microsoft reported the following:

78% of organizations with Microsoft Azure Active Directory (AD) currently do not employ multi-factor authentication (MFA) for their user accounts.[2]

[2]Microsoft Cyber Signals 2022

MFA Datapoint 3: Only 2.5% of Twitter users in the first six months of 2021 used two-factor authentication (2FA)[3]:

The 2.5% usage was split between SMS at 78%, mobile authenticator generator at 30%, and a physical key at 0.5% (some accounts use multiple authenticators).

[3]Twitter Account Security January 25, 2022

These statistics underscore the fact that companies have a long way to go when it comes to securing their customers' accounts with MFA. It is especially surprising that so few Microsoft Azure Active Directory organizations have not moved to any kind of MFA. There appears to be a lack of momentum around making a change to a stronger MFA, or any kind of MFA at all, even in light of a large number of data breaches and account takeovers. This should act as a wake-up call that any movement towards more or better MFA will require strong leadership from fraud experts who can overcome institutional resistance.

Why OTP Is No Longer a Secure Option

Unfortunately, fraudsters have an established playbook to undermine OTPs. Here are a few of the most common attack methods as well as corresponding mitigation options:

Attack Method

SIM Swap Fraud: A fraudster social engineers a mobile carrier employee (typically at a physical storefront) into completing a SIM swap. For some carriers, a SIM swap can also be completed online if there has been an account takeover of the carrier account. Sometimes, the carriers enforce a PIN number that can minimize this type of fraud.

In February 2022, the FBI announced a five-fold increase in fraudulent SIM swaps in 2021.

Mitigation

Select digital identity providers have a direct connection with mobile carriers that allows them to detect when a SIM swap has occurred and alert the customer in under 5 minutes.

Attack Method

Phone Porting Fraud: This is when a fraudster transfers (ports) the phone from one carrier to another. The transfer can also take place within the same carrier. After the port takes place, the customer's phone is dead and any new OTPs will go to the fraudster's mobile phone.

Mitigation

Select digital identity providers have a direct connection with mobile carriers that allows them to detect when a phone port has occurred. Porting can be within a carrier or between carriers. Lapse time to alert the customer is less than 5 minutes after the porting was affected.

Attack Method

SS7 Interception Fraud: This is when a fraudster has a bogus connection with a Signaling System 7[4] (SS7) provider. There are hundreds of small providers with access to the SS7 network and can have the SMS forwarded to the fraudster.

Mitigation

At this time, not much can be done in this situation.

[4]*The Signaling System 7 is an international telecommunication protocol standard that defines how the network elements in a public switched telephone network (PSTN) exchange information and control signals.*

Attack Method

Landline SMS Fraud: Fraudsters can use a service to send an SMS to the landline, but actually divert the SMS to the fraudster without the customer ever knowing.

Mitigation

Use a vendor to identify customer phone type and block an OTP from going to a designated landline.

Attack Method

Sending OTP to an Email Account: A fraudster can easily hijack a customer's email account and receive the OTP.

Mitigation

The practice of email OTP should be immediately discontinued, as it is highly vulnerable, according to NIST.

Attack Method

Sending SMS to VOIP phone numbers

Mitigation

Consider not allowing OTP to go to VOIP phone numbers, especially non-fixed VoIP (typically free). This can be tricky to enforce as the VoIP phone number may be legitimate (e.g., some US service members use VoIP phone numbers from overseas when accessing their financial institutions).

Attack Method

Malware on the victim's mobile phone forwards SMS to the fraudster

Mitigation

One approach here is to use an SMS 'link' type product so that a link is sent to a mobile phone as an SMS, and when the link is clicked by the customer, the system can tell the mobile phone number of the device where the click was initiated. If it is not the mobile phone number where the SMS was sent, it is fraud. Note: Some financial institutions have a policy for no links in an SMS message. Another approach is two-way SMS offered by at least one vendor.

Attack Method

SMS Smishing: A fraudster contacts the customer and pretends to be from a bank and convinces the customer to provide the SMS code when received.

Mitigation

Educate customers that financial institutions will never ask for an OTP code. Also, include text on the OTP SMS message such as "Don't share this secure access code. We will never ask for it."
Note: Social engineering can also occur with OTP codes from authenticator soft token apps (e.g., Google authenticator or SecurID).

The bottom line is that companies must begin moving away from OTPs, passwords, challenge questions, and knowledge-based authentication questions. Until this happens, the attack vectors mentioned above will continue to threaten your customers' accounts and your company's reputation.

What Exactly Is Multi-Factor Authentication?

Now that we've covered some of the ways OTPs can be undermined by fraudsters, let's talk about how to create a robust MFA flow. **The US Government's National Institute of Standards and Technology (NIST) defines MFAs as:**

"Authentication using two or more factors to achieve authentication. Factors include:

- **something you know** (e.g., password/personal identification number (PIN));
- **something you have** (e.g., cryptographic identification device, token); or
- **something you are** (e.g., biometric)." "Multi-factor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors:

"Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously."

In using these authenticators, NIST describes the level of assurance or strength of confidence (see next page) that can be associated with each 'authenticator.' It is at the company's discretion, and possibly its customers, to determine the level of assurance is required at each point where the authenticator is deployed. For example, there may be one level of assurance required for login, but a higher level of assurance required to initiate a real-time wire transaction or transfer $100,000 of Bitcoin to a bank account.

NIST Authentication Levels of Assurance[5]

Authenticator Assurance Level (AAL) 1
AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
Authenticator Assurance Level (AAL) 2
AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two different authentication factors is required through secure authentication protocol(s). **Approved cryptographic techniques are required** at AAL2 and above.
Authenticator Assurance Level (AAL) 3
AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. **AAL3 authentication requires a hardware-based authenticator** and **an authenticator that provides verifier impersonation resistance**; the same device may fulfill both of these requirements. In order to authenticate at AAL3, claimants are required to prove possession and control of two distinct authentication factors through secure authentication protocol(s). **Approved cryptographic techniques are required.**

The level of assurance table above applies only to identity authentication, which typically happens at a later stage after identity proofing has occurred during initial enrollment. To provide a complete picture, it is important to briefly discuss security around the new application/enrollment of a customer, as this occurs before authentications take place. The purpose of identity verification upon enrollment is to confirm the identity of the person enrolling and that they are who they say they are. Because enrollment can span everything from enrolling a consumer in an e-commerce account to a credit card application or a cryptocurrency account, the level of assurance for the identification can vary from limited to all the way up to full Know Your Customer (KYC) US Treasury requirements. Oftentimes, at enrollment, the company/new customer will select the authenticators (including biometrics or platform or roaming authenticators) along with possibly the authenticator public-private keys being set.

[5]*NIST SP 800-63B*

Enrollment also has levels of assurance associated with it (see below).

NIST Identity Assurance Levels[6]

Identity Assurance Level (IAL) 1
IAL1: There is **no requirement to link the applicant to a specific real-life identity.** Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted. Self-asserted attributes are neither validated nor verified.
Identity Assurance Level (IAL) 2
IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing.
Identity Assurance Level (IAL) 3
IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified.

To OTP or Not to OTP? Fortification Is a Short-Term Solution

It's very possible that your company has just implemented OTP or you're interested in deploying more secure options but are just not ready. Assuming your environment supports it, you can set up a quick project to fortify your existing SMS OTP. Some examples of fortifying or strengthening OTP are:

- Using phone-centric or mobile identity signals to verify that the phone number you use for OTP belongs to the customer.
- Using phone-centric or mobile identity signals to validate that the mobile phone number corresponds to the mobile phone being used for the transaction (if applicable).
- Prohibiting non-fixed VoIP phone numbers.
- Leveraging a Trust Score to analyze the reputation and risk of the phone number receiving the OTP. This is also good for detecting recent SIM swap and phone porting.

And remember, there may be some use cases that will always require some form of OTP (e.g., maybe a senior citizen has a landline and a non-smart flip phone).

What To Look for in New MFA Solutions

Now, let's start thinking about selecting one or more new MFA authenticators. While doing this, spend some time upfront assessing your customers' unique needs as well as the risks to the customer accounts and the risk of the transactions. All enterprise customers should be considered high risk, especially web administrators who control other customer access and administrative consoles. On the consumer side, the consumers can range from high net-worth/private banking customers (with several million dollars in online accounts) to small business customers to the general customer base. Now the small business and general

[6] *NIST SP 800-63-A*

consumer base can be doing real-time P2P payments (e.g., Zelle) or retail wires (e.g., $100,000). So, on the consumer side, there can be a need for multiple authenticator types, because there are different levels of risk. One size does not fit all. And maybe the historical physical token still has a role on the retail side.

As a side note, from 2021 to 2022, a number of Singapore banks have been migrating 100% of retail customers from physical tokens to soft token applications. But this year, several banks decided to allow customers to continue to request physical tokens because of a large number of successful and well-publicized SMS scams that were occurring (unrelated to the tokens) and giving customers concern about weak bank security.

The goals for new MFA solutions are:

- Eliminate passwords to prevent data breaches, phishing, and credential harvesting from compromised customer accounts.
- Support **Zero Trust strategies**. This means do not trust the network (assume it is compromised) and put your strong security controls around the authentication step (which can occur continuously during the online session) and limit user access to as little as is needed.
    - The US government just came out with the Federal Zero Trust Strategy in January 2022. In this document, it said Federal Agencies must use strong MFA throughout the enterprise. This includes:
        - MFA must be enforced at the application layer, instead of the network layer.
        - For agency staff, contractors, and partners, phishing-resistant MFA is required.
        - For public users, phishing-resistant MFA must be an option.
        - Password policies must not require use of special characters or regular rotation.
        - When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user.[7]
- Meet the NIST guidelines for the authenticator level of assurance you are striving to achieve.
- Provide a great customer experience and the correct level of assurance with the least friction for the specific authentication event being considered (e.g., login vs a money transfer).
- Address diversity, equity, and inclusion concerns by seeking MFA solutions that minimize bias. Consider differences in user preferences, language, and access to technologies. E.g., ensure the solution works well for the 65+ age group and customers with disabilities.
- Provide a proper level of assurance for maintenance transactions (e.g., change user ID, change phone number, unlock user from the account). Don't fall back to passwords or OTP for account maintenance. Your stronger authentication for login and transactions is only as good as the authentication allowed on maintenance activity.
- Prevent authentication bypass, where fraudsters can use malware and grab cookies, session data, etc. and simply skip the authenticator and go to the first post-authentication screen.
- Incorporate mobile device data points in the authentication solution. Since the mobile phone is such a critical user device going forward, be creative on how you add security around mobile transactions. There are so many security data points that can be accessed on a phone (e.g., geolocation, rooted/jailbroken, mobile phone is stationary, battery at 100%, etc.).

[7]*The Federal Zero Trust Strategy is published as OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" January 26, 2022*

MFA Migration Considerations

There are several ways to migrate to MFA. First, there are a number of vendors that offer complete MFA solutions. Second, there are standards, such as FIDO2/WebAuthn, that document how to build out new MFA solutions. When deciding whether to partner with an MFA vendor or build out your own MFA solution, be sure to consider the following:

- Some of the vendors have actually used FIDO2/WebAuthn standards to fully build their MFA solutions. One of the potential benefits of a fully built-out solution could be a better customer experience because there are a number of companies using the same solution. At a minimum, you can see the entire UX and make your own assessment as to how good the customer experience will be. Plus, this approach makes it easier to test the flows early on.
- Building your own MFA solution can allow customization of the authenticators and the flows. This will probably take more time and possibly introduce the potential for more security risks if the coding is not done correctly.
- Regardless of whether you build a solution or partner with a vendor, the solution must address both desktops and mobile devices. For instance, a customer may have an Intel PC, an iPad, and an Android or IOS phone and the MFA solution needs to allow the customer to logon on to any of these devices and execute transactions. So, make sure you assess your MFA solution with a number of mobile devices (phones and tablets) and personal computers (PCs and Macs), and different operating systems/versions and ages of devices. For example, some Apple iMacs and MacBooks don't have a Trusted Platform Module (TPM) and therefore don't support FIDO2. On the other hand, in October 2021, Windows introduced the Windows 11 operating system. Windows 11 requires the TPM to be active on the device.
- You also need to assess the impact of platform operating system upgrades and browser upgrades to understand how these changes can impact the execution of the authenticators.
- The solution must also address the fact that devices get stolen, lost, and replaced. So there has to be a way to bridge from existing devices to new devices and still maintain the MFA authenticators.
- One concept that can help with personal computers is that once the mobile phone is set up and authenticated, it can be used to authenticate the setup of the second and third devices. The mobile phone can also be used to authenticate web transactions.

A Word from FIDO

The FIDO Alliance is an "open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation."

In February, FIDO came out with a concept document identifying two key achievements they are working towards:

- "The ability to use a phone as a roaming authenticator through a defined protocol to communicate between the user's phone (which becomes the FIDO authenticator) and the device from which the user is trying to authenticate."
- "Making FIDO credentials universally available on all the user's devices to ensure they can survive device loss and sync across different devices."[8]

[8]*Charting an Accelerated Path Forward for Passwordless Authentication Adoption, Andrew Shikiar, executive director and CMO, FIDO Alliance, March 17, 2022*

Watch out for vendors that have a really good MFA solution for mobile but are weak or have not really thought out the web component of MFA.

Types of MFA Authenticators

There are a number of MFA authenticators that can be used. Some of these include:

MFA Authenticators
Mobile phone
Physical token (e.g., RSA SecurID hardware token, OneSpan Digipass device)
Mobile app TOTP code generator (e.g., Google Authenticator, Microsoft Authenticator, RSA SecurID Software token)
Physical Security Key (e.g., Yubico Yubikey, Google Titan security key). This is known as a Roaming authenticator in FIDO2/WebAuthn. This key is typically attached to a device via the USB port, Thunderbolt port, or Lightning port.
Push Notification to a mobile app
Platform authenticator (web or mobile) with a virtual security key and a biometric (e.g., Windows Hello and Apple's Touch ID)

When looking at Platform and Roaming authenticators for FIDO2/WebAuthn, this WebAuthn link shows the availability of authenticator usage by the operating system and browser. There are currently some limitations.[9]

As previously mentioned, a good solution design may need to include a number of authenticators depending on the type of customers (e.g., private banking vs. consumer, commercial users) and the level of authorization the various users have to more risky parts of the online services (e.g., web administrators).

Note: *NIST recommends that a biometric authenticator should always be incorporated with a second factor. As a result, we are seeing biometrics commonly offered as part of an authenticator. An example of this is a fingerprint reader on a Yubico key.*

Here is a good tip for getting familiar with authenticators: experiment with a myriad of authenticators (Google Authenticator, Yubico key, facial biometrics, etc.) in your personal online environments (e.g., Gmail, Facebook) to fully understand the client experience and potential shortfalls around enrollment and use across the user journey. There are twists on how authenticators work (e.g., what happens to Google Authenticator when you get a new phone?).

[9] https://webauthn.me/browser-support.

Behavioral Biometrics

A comprehensive MFA solution should provide continuous authentication across the online session. The ideal situation is that the security solution always knows who is doing the activities after the login. One way to achieve this is with behavioral biometrics.

Behavioral biometrics is not a one-size-fits-all type of solution. There are many components of a good behavioral biometrics solution that can come into play during an online session. It is a layer of security that can passively verify a user during a transaction.

There are also some compelling examples of behavioral biometrics being used to identify and prevent consumers from completing transactions under the false pretenses of fraudsters.

So, in the case of continuous authentication, behavioral biometrics can help passively authenticate the user without introducing friction. Also, the security key component of a platform authenticator (both web and mobile) can be passively checked throughout the session. Additionally, signals from a mobile phone can also be used passively during the session to confirm the user has not changed. With these examples, the aspect of passive continuous authentication helps keep friction to a minimum during the online session and may mitigate the need for additional in-session active authentication.

Guidelines for Deploying MFA

There are some important deployment considerations when you roll out MFA.

Understand the Implications of MFA Bypass

First, make sure you understand the implications of MFA Bypass. MFA Bypass is the ability of the fraudster to get around the authentication step and be considered authenticated. If the MFA solution is not integrated correctly, fraudsters might be able to bypass the authenticator.

So, this means you need a strong online security infosec individual, or external expert, to be part of your team to complete the Authenticator Bypass Threat Assessment. The bypass threat can occur because of weak coding surrounding the MFA or new attack vectors that can make the authenticator inherently weak. So really understand Bypass risk before selecting the authenticator. Bypass risk is very real. Several recent data breaches involved bypassing MFA:

> "As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA protocols. Russian state-sponsored cyber actors successfully exploited the vulnerability while targeting an NGO using Cisco's Duo MFA, enabling access to cloud and email accounts for document exfiltration."[10]

Note: This InfoSec professional can also be key in assessing the security/cryptography of the MFA itself (e.g., how secure is the transport of the push notification to the mobile app, how secure are public/private keys that are part of the platform authenticators or can the roaming security key be defeated by malware residing on a PC?).

[10]*Russian State-Sponsored Cyber Actors Exploit Default MFA Protocols, Alix Pressley, March 17, 2022*

Customer Experience Is Critical

Remember that customer experience is critical to customer acceptance and adoption so be sure to have some good UX experience on your team. The customer experience involves both the set-up of the authenticator ("enrollment") and the actual ongoing usage of the authenticator. Also, test your solution with internal staff and then do a limited pilot with real customers before any rollouts. This will make or break your deployment. An interesting usability study worth reviewing is called "A Usability Study of Five Two-Factor Authentication Methods."[11]

As you think about the customer experience, consider the customer journey from enrollment and selecting authenticators through logon and executing financial transactions. Authenticator enrollment should be intuitive for everyone in your diverse customer base. You want as much of the authentication process (at enrollment and logon/transaction) to occur behind the scenes (e.g., the use of cryptographic keys, checking mobile geo-location, platform authentication on Windows PCs, etc.) while providing enough transparency to the customer that the authentication is secure.

Address Account Recovery

A solid MFA solution needs to address account recovery (e.g., password reset, user ID locks, and other customer maintenance issues). Otherwise, you may still have weak authentication for these maintenance activities. This is what FIDO said in February on account recovery in regards to the current FIDO2/WebAuthn standards:

> "So, what happens to your FIDO login credentials, and how do you recover your account if you change your phone or laptop? They are not recoverable in today's FIDO model. This presents issues for deploying FIDO at scale to consumers who are constantly moving between devices and updating to new ones."
>
> "….help service providers bring passwordless sign-in to consumers at scale by addressing the issue of account recovery – the key barrier to mass adoption of cryptographically secure, passwordless authentication."[12]

Tip: Since FIDO2/WebAuthn is still working on account recovery, some vendors have ways to improve your existing controls around account recovery in the interim.

Consider Challenge Orchestration Software

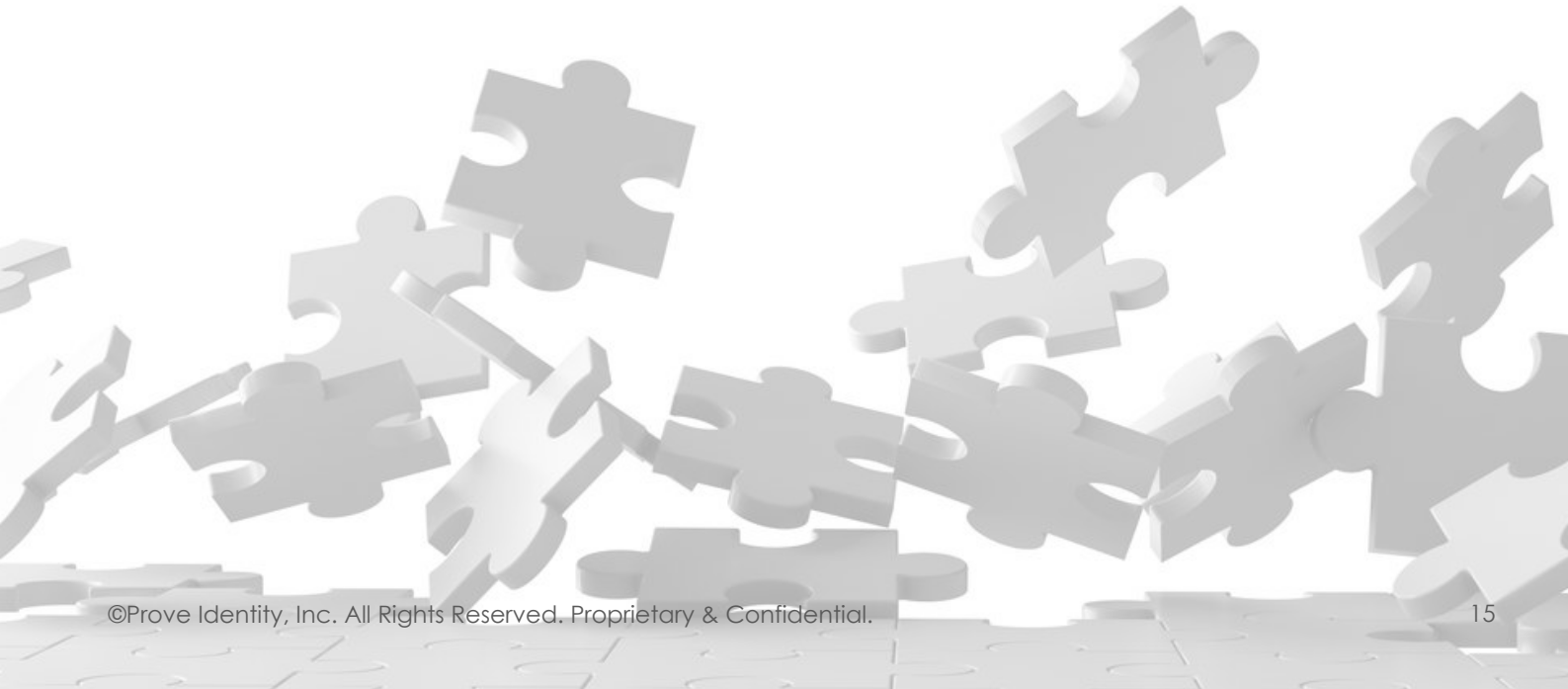
Finally, to manage the authenticators and the various transactions, you should consider a challenge orchestration software component to coordinate the timing and use of the various authenticators across all of the online session events. This can help get your MFA solution to market quicker. Plus, with FIDO2 WebAuthn, the authenticators can be tied to devices, browsers, and operating systems. Orchestration software can help control this mix of data points. There are a number of vendors that offer challenge orchestration solutions and these vendors will often offer pre-built MFA authenticators. Challenge orchestration software can be multi-purpose solutions that can help with other orchestration such as orchestrating the fraud controls used in online account opening.

[11]*Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, Kent Seamons, Brigham Young University 2019* https://www.usenix.org/system/files/soups2019-reese.pdf

[12]*Charting an Accelerated Path Forward for Passwordless Authentication Adoption, Andrew Shikiar, executive director and CMO, FIDO Alliance, March 17, 2022*

MFA Checklist

Does the solution…
eliminate passwords to prevent data breaches, phishing, and credential harvesting?
support Zero Trust strategies?
meet the NIST guidelines for the authenticator level of assurance you are striving to achieve?
provide a great customer experience and the correct level of assurance with the least friction for the specific authentication event being considered (e.g., login vs a money transfer)?
address diversity, equity, and inclusion concerns by seeking MFA solutions that minimize bias?
provide a proper level of assurance for maintenance transactions?
prevent authentication bypass?
incorporate mobile device data points in the authentication solution?
work with multiple types of MFA authenticators?
leverage behavioral biometrics?



Summary

This MFA Buyer's Guide has provided the following information:

- A recent history of authenticators
- How to strengthen your OTP authenticator while you work to replace it with a better MFA
- Goals for new authenticators
- A discussion of the key considerations for selecting and deploying MFA solutions/authenticators

Remember, the goal of adding MFA should be to improve security while providing the best possible customer experience. A great customer experience will be imperative for a successful project.

Encouraging customers to adopt the new MFA process will require educating customers on its many benefits. Both better security and a great customer experience take time to get right.

Be sure to leave time for trial and error as this is not a sprint but rather a journey.[13]

Finally, rest assured you will be in good company as you begin this journey. A number of financial institutions have already deployed advanced MFA (advanced MFA can include passwordless, phishing resistant, Zero Trust, FIDO2/WebAuthn, etc.) and a number of other companies are already in the research/planning phase.

If you or your company are reluctant to begin this journey, please keep in mind that cyber insurance companies are starting to make MFA a requirement for new policies. Simply put: no MFA, no cyber insurance.

Authors

Ken Palla
Advisor, Palla Consulting
Former Director, MUFG Union Bank

Patrick Merfert
VP of Product Marketing at Prove

Bill Fish
VP of Authentication at Prove

Fitzwilliam Anderson
Strategic Content Editor at Prove

You may have questions after reading this white paper on the many benefits of bolstering your MFA. Reach out to one of our fraud specialists today to learn how to fortify your company's security, prevent fraud, and improve user experience with Prove's solutions.

Speak to an Expert

Prove

[13] *Take the time to read the information made available by NIST for online security. primarily SP 800-63A, B, and C (https://csrc.nist.gov/publications/detail/sp/800-63/3/final). Also, visit The FIDO Alliance website (www.fidoalliance.org) for more detailed information on FIDO2 and WebAuthn. The FIDO Alliance regularly hosts meetings and webinars that discuss this standard and describe real-world implementations.*

Prove Auth™: Go Passwordless

Prove

Move beyond passwords and OTPs with a 1-tap authentication solution.

Multi-Factor Authentication (MFA) needs to evolve.

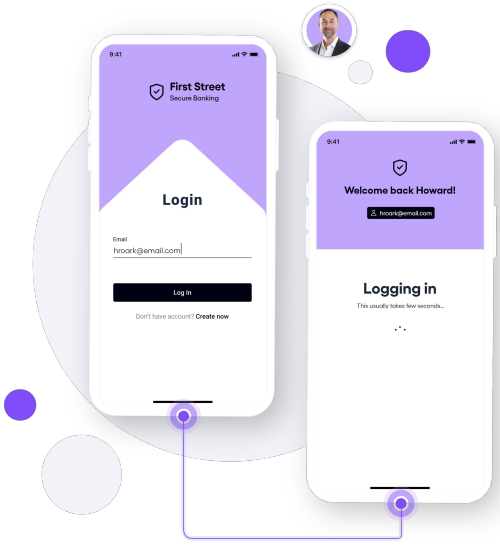
Businesses want to improve onboarding experiences, reduce costs and improve outcomes, but legacy MFA has drawbacks:

- **Passwords and OTPs are vulnerable** to social engineering and other fraud vectors
- **Friction negatively impacts** consumer experience and revenue
- **Password Resets & OTPs are costly**

Prove Auth *already has.*

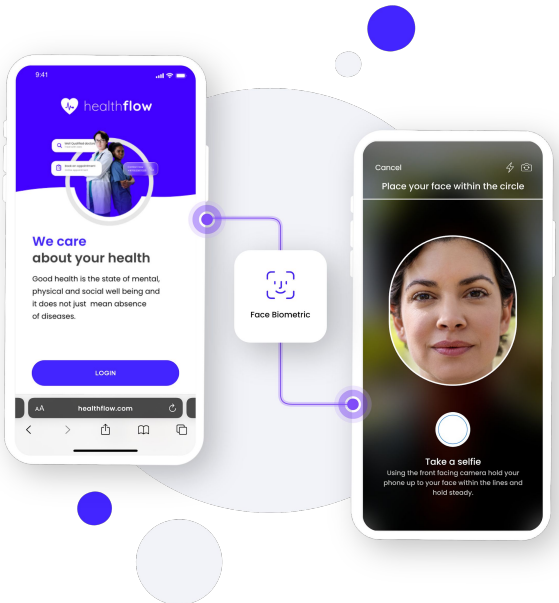
A unified solution for passwordless login, omnichannel authentication, and/or a seamless second factor. With Prove Auth, companies can:

- **Reduce reliance on OTPs and passwords** with 1-tap login or step-up authentication
- **Authenticate any device, anywhere** via app push notification or biometrics
- **Reduce authentication costs** by cutting out OTP and password reset charges



Go Passwordless!

Prove Auth enables passwordless authentication for mobile apps and omnichannel experiences and protects from fraud and account takeovers — all while enhancing the consumer experience.



No App? No Problem.

Deploy Prove's FIDO2 web-based authentication. Authenticate directly with Prove or utilize on-device biometrics for step-up measures — no need for clunky apps or passwords.

Case Study

Tier 1 Financial Services Firm

CHALLENGE:

Prior to Prove, consumers manually entered all personal data for credit card applications which added friction and led to high abandonment rates.

SOLUTION:

Client integrated **Prove Pre-Fill,** including **Prove Auth** authenticators for initial possession check, to provide a seamless application experience while decreasing abandonment and stopping bad actors. With just the consumer's phone number and last 4 of SSN, the credit card application is auto-filled with authenticated data.

RESULTS:

$800M
Increase in Annual Sales

75%
Reduction in Fraud Rates

Key Benefits

- Seamless authentication reduces friction and removes social engineering risk (no OTPs to steal)
- Replaces OTPs with new methods that reduce reliance on MNOs
- The combination of capabilities allows for authentication to be initiated in any channel
- Unlimited-use pricing creates cost savings with every user authentication over OTP

Key Differentiators

- Integration with Prove's Pinnacle platform creates strong confidence in the identity behind the authentication
- Cryptographic keys establish on-device credentials, creating a strong bind between phone and user
- Cryptographic keys enable silent, out-of-band authentication in any channel while reducing opportunity for social engineering

Prove

1,000+ companies and **500+** banks trust Prove to secure their onboarding, digital servicing, call center, e-commerce, payments, and compliance experiences.

Ready to supercharge your customer onboarding?
Learn more at: www.prove.com/contact

Aite Novarica — Fraud & AML Impact Innovation Award

Expert Insights — Best of Multi-Factor Authentication

Gartner — Cool Vendor

5 years in a row

Technology Fast 500
2021 NORTH AMERICA
Deloitte.