Prove

REPORT

2023

State of MFA Report

As consumers continue to use digital services and create online accounts at an accelerated pace, the usage of multi-factor authentication (MFA) has become more prevalent as a way to secure transactions. However, consumer attitudes towards MFA continue to change as it becomes a more mainstream concept and service, and as more frictionless and secure identity authentication options emerge. Prove sampled 1,000 US adults in a series of surveys to get a better understanding of security measures they take online and their perspectives on MFA. The survey reveals five key findings:

Key Findings

1. **Consumers desire more streamlined authentication options**
2. **MFA adoption rates vary significantly by service/industry**
3. **MFA in the workplace continues to lag**
4. **Consumers recognize the importance of strong identity authentication processes.**
5. **Consumers don't want to pay for MFA**

Before we dive deeper into the survey data that led to these key findings, let's briefly review what MFA is and what some of the major challenges are. Skip ahead to the survey results if you're already familiar with these basics.

What is Multi-Factor Authentication?

Multi-factor authentication is a security method that requires two forms of evidence, or credentials, to be presented during the login process. This additional layer of security is recommended by the National Institute of Standards and Technology ("NIST") to help protect against unauthorized access to accounts. MFA requires two out of the following three types or classifications, also referred to as "factors of authentication," in order to be securely authenticated:

- Something you ***know***, such as a password or PIN
- Something you ***have***, or possess, such as a badge or smartphone
- Things you ***are***, such as a biometrics (fingerprints or face recognition)

Examples of employing 2 factors of authentication to achieve MFA include entering a one-time passcode sent via SMS (e.g., 894563) after entering your username and password for your bank account, or undergoing a face scan after entering your username and password for your brokerage account. While MFA has been used in older technologies such as the ATM, it is now becoming increasingly prevalent online. Logging into social media, accessing email from an unfamiliar device, and ordering food online often require some form of MFA process.

What are the downsides of multi-factor authentication?

Two of the major challenges of traditional MFA offerings, such as email or SMS OTPs, are security vulnerabilities and end user/consumer friction. Let's discuss potential security vulnerabilities first.

What are the potential security vulnerabilities associated with MFA?

Although MFA often adds a critical layer of security, not all MFA is created equal. For example, one of the most common forms of MFA, the one-time passcode, is frequently intercepted by fraudsters through account takeover methods such as SIM swap attacks or porting attacks.

What are the negative impacts of friction on MFA?

Security flows that add too much friction to the user experience, meaning they are tedious, time-consuming, and frustrating, drive away consumers. Even something as simple and ubiquitous as the username and password can frustrate users who are eager for easier alternatives. According to Prove and OnePoll's 2022 Passwordless & Authentication Consumer Trends Report, 62% of respondents wanted an option to ensure their data is protected that is *not* traditional MFA, and 64% of respondents said that authentication through their phone is a more convenient option than passwords.

Here are the 5 key findings from the survey:

Key Finding #1:

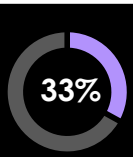
Streamlining MFA experiences is key to increasing adoption rates

While enabling MFA is important when creating and accessing online accounts, it can be a tedious process for consumers. Enabling next generation MFA that removes OTPs, and even passwords in certain cases, will create a seamless experience for consumers while also protecting them and the organizations they work for.

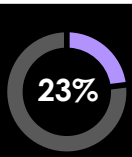
- **33%** of consumers said they do not enable MFA because they find it to be an annoying process
- **23%** of consumers said they don't enable MFA because it is too slow and **36%** of consumers think that MFA should take ten seconds or less
- **58%** of consumers believe that companies should deprecate passwords altogether and use more secure technology such as mobile-based authentication
- **62%** of consumers said they wanted an option that isn't MFA to ensure the security of their data

In light of how busy consumers are, creating MFA flows that are seamless, secure, and free of friction is key to boosting revenue and preventing fraud.

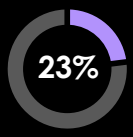
What are the top reasons survey respondents do not enable traditional MFA?



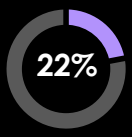
It's annoying



It's too complicated



It's too slow



Verification often gets lost in spam or not delivered at all

Key Finding #2:

MFA adoption varies significantly by service/industry.

From home to the workplace, MFA has become a common security practice to ensure that accounts cannot be accessed by bad actors and that sensitive data is stored securely. While it is expected that users would rely on this service to protect themselves across accounts, consumers may not be enabling multi-factor authentication in the areas you may think.

When given an option…

- **73%** of consumers do not enable MFA for cryptocurrency accounts
- **70%** of consumers do not enable MFA when using social media
- **80%** of consumers do not enable MFA when online gambling
- **77%** of consumers do not enable MFA when using streaming services

Considering just how frequently fraudsters target crypto accounts and online gambling for account takeovers and hack into social media accounts to conduct phishing attacks, it's clear that consumers are taking a major risk by not enabling MFA when given the option.

On the other hand, MFA is more popular among consumers for other online services, including:

- **60%** of consumers enable MFA for online banking
- **61%** of consumers enable MFA for online healthcare portals and apps
- **60%** of consumers enable MFA to access insurance accounts

Considering the highly sensitive data contained in such accounts, it's heartening to know that the majority of users would enable traditional MFA voluntarily for these types of accounts. That being said, a sizable portion (~40%) still would rather risk fraud than deal with the added friction of existing MFA flows.

Key Finding #3:
Multi-factor authentication in the workplace continues to lag

With the shift to remote or hybrid models of work following the COVID-19 pandemic, improving security measures for work devices has become absolutely critical as more and more business is conducted outside the secure confines of the office. Unfortunately, the survey results showed that:

- Only 21% of consumers use MFA more on work accounts than they do on personal accounts
- Less than half (48%) of employers mandate that employees use MFA at work
- Only 19% of consumers have to use MFA across work accounts

Considering the devastating effects a fraud event can have on a business's bottom line and reputation, increasing MFA usage for employees is of paramount importance. When doing so, however, companies should consider next generation MFA solutions.

Key finding #4:
Customers recognize the importance of strong identity authentication processes

It's true. In today's digital-first world, customers are finally recognizing just how important strong identity authentication truly is. In fact, the majority (53%) of customers said they would switch financial institutions based on the strength of their identity authentication processes.

Key finding #5:

Customers don't want to pay for MFA

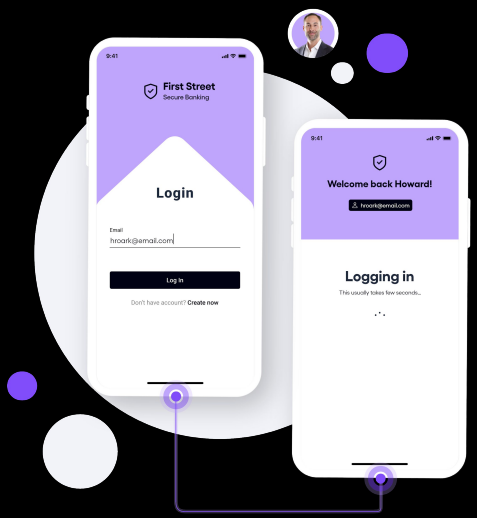
A staggering 87% of consumers think that MFA should be free, as opposed to a paid service. This makes sense in light of the recent debate around Twitter's decision to charge for 2FA, and given that all consumer-facing businesses should prioritize and invest in the protection of their customers.

Final Words

Even amid the current spike in fraud, the 2023 State of MFA Report reveals that consumers still prioritize user experience above all else. Fortunately, with the latest generation of digital identity technology hitting the market, companies don't need to choose between security and user experience.

"As we have all seen, the security that online businesses use is overly tedious and yet not very secure," said Prove Chief Executive Officer Rodger Desai. "The bottom line for consumers? Complicated doesn't mean secure. The solution is actually sitting in the pocket of most adults – their cell phones. With Prove, your phone becomes by far the most secure, accurate, and frictionless way to prove identity – and our survey demonstrates that consumers would prefer the convenience of the phone in their pocket."

Rodger Desai, Chief Executive Officer
and Co-Founder of Prove



Meet Prove Auth.

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

- **Reduce reliance on passwords and OTPs** with passwordless login or step-up authentication
- **Authenticate any device, anywhere** via app push notification or biometrics
- **Reduce authentication costs** by cutting out OTP and password resets charges and enabling simplified re-binding of new devices using behavioral models

To learn more about Prove Auth and how you can gain a competitive advantage by streamlining the consumer authentication experience while also preventing fraud, **request more info or speak with an expert here.**

Prove