


Multi-Factor Authentication Research Read-out

October 2022

Agenda

- 
1. Goal and methods
 2. Customer support data
 3. Quantitative analysis
 4. User research findings
 5. Next steps

1 / Goal and methods

Our goal is to help members of the public easily create and sign in to a secure account to access government services.

Questions to answer

- What have been the major pain points with multi-factor authentication (MFA)?
- Where are users running into issues?
- What kinds of issues?
- What are the contributing factors?
- What authentication methods are the most effective?
- What groups of users are affected by these major pain points?

How we answer these questions

Ongoing research and analysis of our current authentication flow:

- Iterative research and usability testing
- Customer support ticket analysis
- Quantitative drop-off analysis

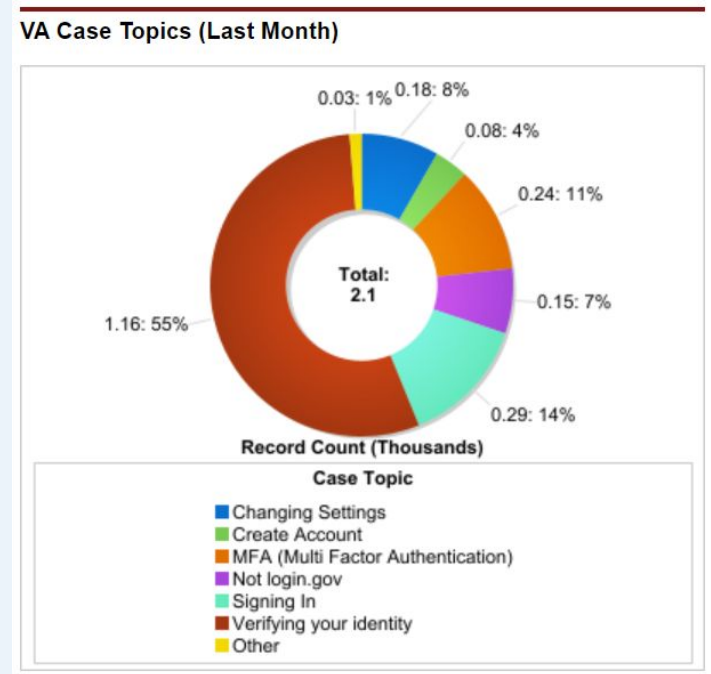
Upcoming research:

- Direct observation study in partnership with VA
- Jobs To Be Done framework for Login.gov users

2 / Customer support data

**“Multi-factor Authentication” and
“Signing In” make up a combined
25% of case topics.**

Identity verification remains the biggest issue for VA users, at 55% of case topics.



Case topics for MFA for VA, September 2022

Face or Touch Unlock and PIV/CAC are the biggest MFA sub-topics for VA users.

Case Sub Topic	Cases
Face or Touch Unlock	82
PIV/CAC	53
Lost MFA method	32
No OTP received	19
Invalid OTP	18
Authentication app	10
Backup codes	9
International number	5
Other	5
Security Key	3
New Device Notification	1
Unwanted OTP sent	1
Personal Key Notification	1
Multiple OTPs sent	1
Grand Total	240

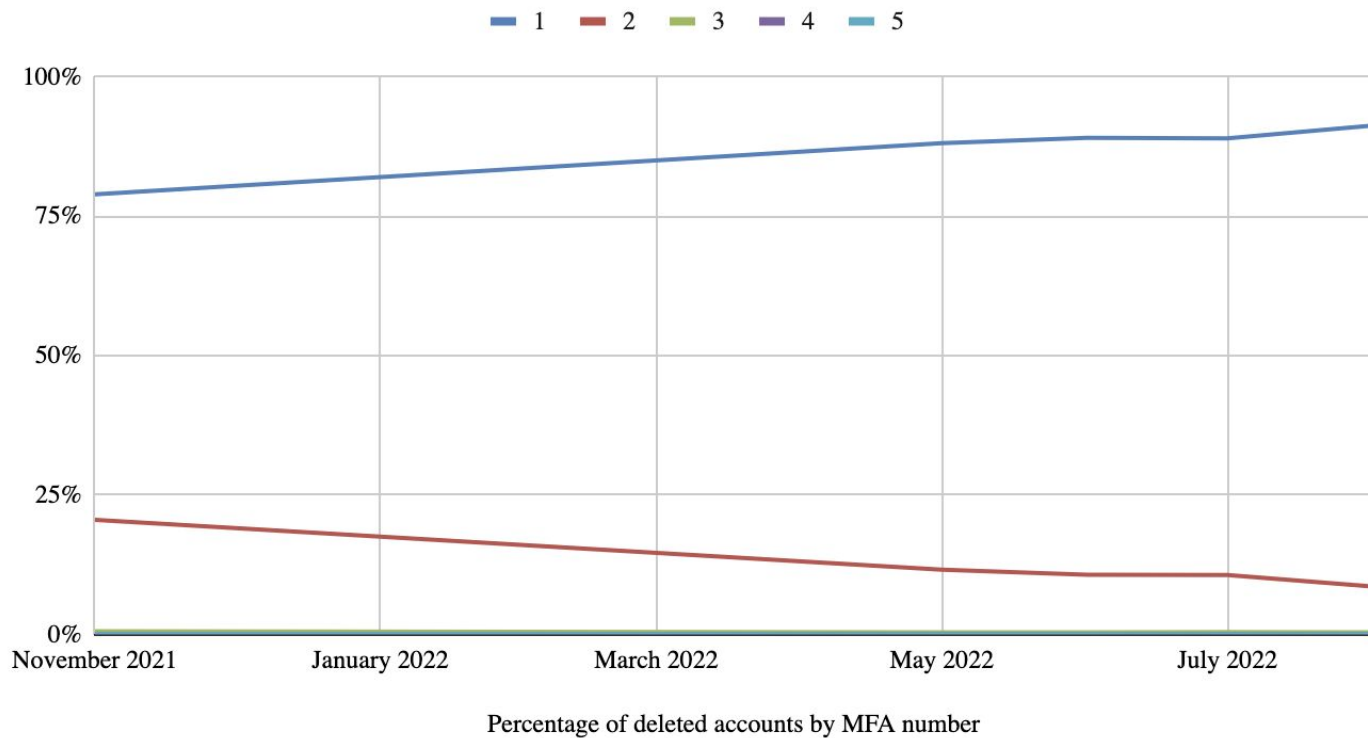
Case Sub Topic	Cases
Need More Information from Customer	133
Recover Account	48
Locked out	35
Other	32
Forgot password	27
Invalid Personal key	4
Remember device issue	3
Backup codes	2
Bug	1
(blank)	1
Site navigation	1
Grand Total	287

3 / Quantitative analysis

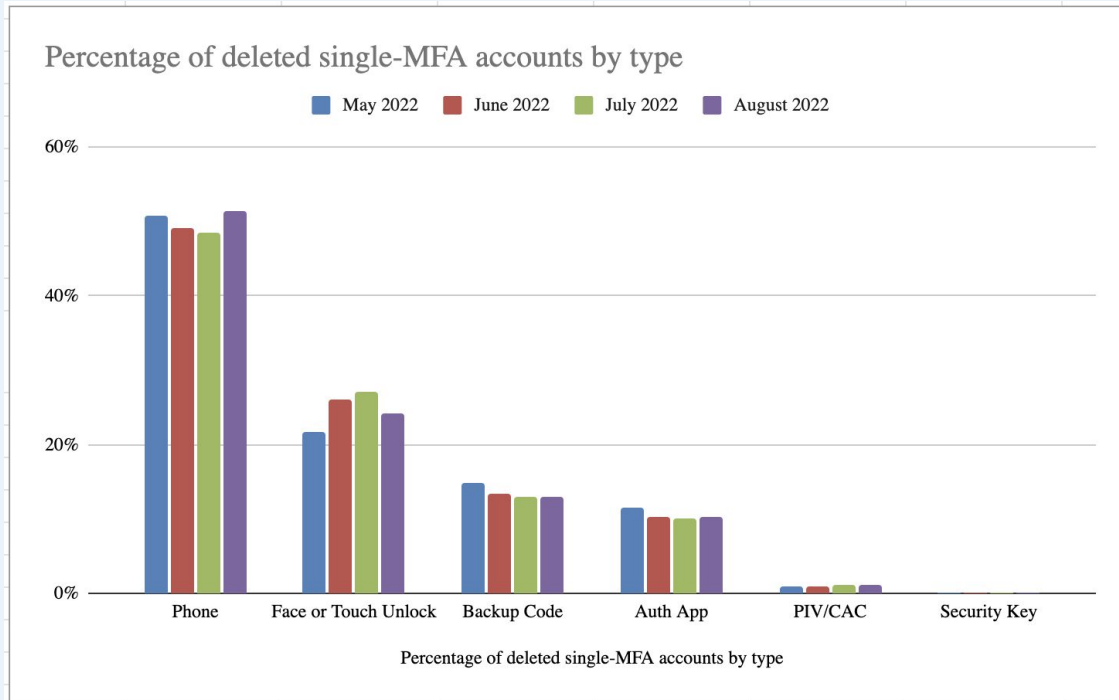
Users who have only one MFA method set up are most likely to lose access to their account.

If users only have one MFA method set up and they lose it, they are unable to sign in and have to delete their account.

Number of MFA on Deleted accounts by Percentage



Users with only Phone MFA set up make up the majority of deleted accounts, followed by Face or Touch Unlock.



Percentage of total new accounts (August 2022):

Phone = 82%

Face or Touch Unlock = 8%

Backup codes = 1.5%

Authentication app = 4%

PIV/CAC = 2%

MFA methods tied to a device are more secure, but are easier to lose access.

Phone/SMS is more phishable, but can easily be used between devices.

Backup codes may be more or less secure, but are easy to lose.

Security keys, authentication apps, and PIV/CAC are all more secure, but rely on the user's access to a single physical device and/or application.

Face or Touch Unlock (Platform Authentication) is bound to a specific device, but updates are being made to make cross device access.


4 / User research findings

Login.gov conducts iterative user research to help users set up multiple MFA methods and feel more secure and confident in their choices.

January 2022

Authentication method setup

Add a second layer of security so only you can sign in to your account.

 Keep this information safe. You will be locked out and have to create a new account if you lose your authentication method.

Select an option to secure your account:

☐ **Security key**

Use a security key that you have. It's a physical device that you plug in or that is built in to your computer or phone (it often looks like a USB flash drive). Recommended because it is more phishing resistant.

MORE SECURE

☐ **Government employee ID**

Insert your government or military PIV or CAC card and enter your PIN.

MORE SECURE

☐ **Authentication application**

Get codes from an app on your phone, computer, or tablet. Recommended because it is harder to intercept than texts or phone calls.

SECURE

☐ **Phone**

Today

Authentication method setup

Add another layer of security by selecting a multi-factor authentication method. We recommend you select at least (2) two different options in case you lose one of your methods.



Face or touch unlock

Your device scans your face or fingerprint and confirms the information is a match to the images you already have stored on your device. We do not copy or store these images.



Government employee ID

PIV/CAC cards for government and military employees. Desktop only.



Security key

A physical device, often shaped like a USB drive, that you plug into your device.



Authentication application

Download or use an authentication app of your choice to generate secure codes.



Text or voice message

Receive a secure code by (SMS) text or voice call to your device. Do not use web-based (VOIP) phone services or premium rate (toll) phone numbers.



Backup codes

A list of 10 codes you can print or save to your device. When you use the last code, we will



A phone was added to your account.



You've added your first authentication method. Add a second method as a backup.

Adding another authentication method prevents you from getting locked out of your account if you lose your only authentication method.

Add another method

[Skip for now](#)

When offered the option to select more than one authentication method, 58% of participants said they would select at least two MFA methods.

38% of participants added a second MFA method when they saw another encouragement prompt.

In two rounds of research, all participants set up Phone/SMS.

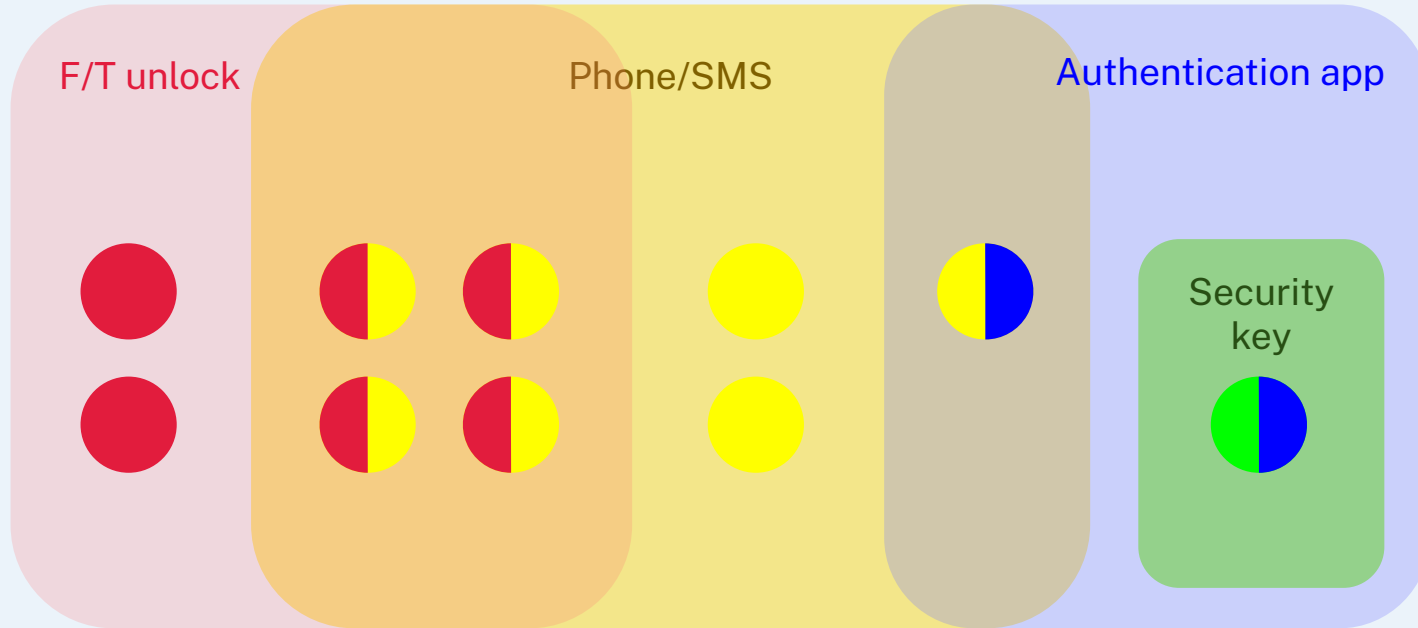
In Round 1, participants could choose to set up one or two authentication methods.

- 83% of participants set up **Phone/SMS** as their first, primary MFA method
- 58% ended up with **Phone/SMS** as their only method
- 42% selected **Backup Codes** as their secondary MFA method
- 25% attempted to set up an **Authentication application**, but failed to authenticate

In Round 2, all participants were prompted to set up two authentication methods.
For their additional method:

- 70% of participants chose **Backup codes**
- 20% of participants chose **Authentication application**
- 10% of participants chose **Face/Touch unlock**

Authentication method preferences from Platform Authentication Sentiment Analysis



60% of participants expressed skepticism about sharing biometric data and lacked trust in the message “We do not store your fingerprints or images.”

80% of participants had no issues or confusion with setting up Face or Touch Unlock for the first time on their device or with a prototype.

70% of participants did not understand how Face or Touch Unlock worked if Login.gov did not collect their biometrics.

“

I'm curious to know how do you know it's my face or fingerprint if you don't keep my face or fingerprint in your files? Or is that a government secret?"

“

This says 'we do not store your fingerprints or images.' So how do they know you're using the right fingerprint?"



Use your device

Enable face or touch unlock as an authentication method on this device. You'll need this device to use this method in the future. We do not store your fingerprints or images.

Start by giving your device a nickname.

Device nickname

My Device

☒ Remember this browser

Continue

[◀ Choose another option](#)

70% of participants preferred Option B



Face or touch unlock

Your device sends us a confirmation that you are the person accessing your account. We do not store images of your fingerprint or face.

A

Face or touch unlock

Your device scans your face or fingerprint and confirms the information is a match to the images you already have stored on your device. We do not copy or store these images.

B

80% of participants preferred Option B

A

Use your device

Your device sends us a confirmation that you are the person accessing your account. We do not store images of your fingerprint or face. You'll need the same device to sign in using face or touch unlock in the future. [Learn more](#)

B

Use your device

When you want to access your Login.gov account, you use your device to scan your face or fingerprint. Your device confirms if those scans are a match to ones stored on the device. We do not store images of your fingerprint or face. You'll need the same device to sign in using face or touch unlock in the future. [Learn more](#)

Prompting users to set up more secure methods



Additional authentication required

This app requires a higher level of security. You need to verify your identity using a physical device such as a security key or federal government employee ID (PIV or CAC) or an authentication application to access your information.

Select an option to secure your account:

☐ **Authentication application**

Get codes from an app on your phone, computer, or tablet. Recommended because it is harder to intercept than texts or phone calls.

☐ **Security key**

Use a security key that you have. It's a physical device that you plug in or that is built in to your computer or phone (it often looks like a USB flash drive). Recommended because it is more phishing resistant.

☐ **Government employee ID**

Insert your government or military PIV or CAC card and enter your PIN

Authentication method setup

This app requires a higher level of security. You need to verify your identity using a physical device such as a security key or federal government employee ID (PIV or CAC) or an authentication application to access your information.

Select an option to secure your account:

☐ **Authentication application**

Get codes from an app on your phone, computer, or tablet. Recommended because it is harder to intercept than texts or phone calls.

☐ **Security key**

Use a security key that you have. It's a physical device that you plug in or that is built in to your computer or phone (it often looks like a USB flash drive). Recommended because it is more phishing resistant.

☐ **Government employee ID**

Insert your government or military PIV or CAC card and enter your PIN

36% of participants understood the description of authentication apps, but 27% of participants were confused.

Two participants thought that authentication apps included email and SMS authentication. Two participants thought that the app would be specific to Login.gov or the agency.

“

Is this an app that is specific to authentication on this website, or authenticating anywhere?

“

What is the app? I have no idea what app I would use.

73% of participants had never heard of security keys.

Three participants had heard of security keys, but two of them mentioned that security keys would generate codes.

“

I wouldn't use a security key because it's easy to lose something physical, unless it's in your computer.

“

Is this something I can go to Staples and buy? Do they sell security keys? I have no idea.

3 / Next Steps

Next steps

- 1** Login.gov/USDS and VA to partner on upcoming research to continue improving the MFA experience
(Direct Observation Study)
- 2** If interested, Login.gov can host a collaborative workshop with VA to analyze customer support tickets
- 3** VA to continue research on security keys and pilot new initiatives for increasing secure MFA adoption
- 4** Login.gov can pull additional MFA statistics that are specific to VA

Questions?