

Collect Multi-Factor Authentication (MFA) Quick Reference Guide

CFPB is enhancing our cyber and data security through multi-factor authentication (MFA) for all systems accessed by external users.

Starting in March 2023, Collect began requiring users to go through an MFA process when logging into their accounts. This means that users have to provide additional information or credentials, apart from their username and password, to access their Collect accounts.

MFA is a security technique that verifies a user's identity by requiring them to provide multiple pieces of information or credentials. In practice, this means that when you log into your Collect account, you will be prompted to enter a code sent to your registered device, answer security questions, or use an authenticator app.

MFA is a vital security measure that protects your account from unauthorized access or cyber-attacks. Collect encourages all its users to take advantage of this feature and ensure that their accounts are as secure as possible.

MFA Overview

What is MFA?

MFA is a way for Collect users to securely log into the site that requires using "factors" to verify (authenticate) who they are before gaining access. With MFA, users must use at least two or more "factors" to log in. These factors can be:

- **Something You Have:** Something that only the user possesses to login, such as a token from an authentication app on a mobile device or a hardware security device.
- **Something You Know:** A password or PIN.
- **Something You Are:** Biometrics, such as a fingerprint scan or facial recognition.

Why is CFPB requiring MFA?

MFA is an essential tool that organizations and individuals can use to help protect against cyber threats. President Biden issued an [Executive Order on Improving the Nation's Cybersecurity](#) on May 12, 2021, directing federal agencies and departments to improve cybersecurity, including rapidly implementing MFA across their enterprises. The administration then provided more specific MFA guidance in the federal Zero Trust Strategy ([M-22-09](#)).

CFPB is serious about implementing MFA and making the login process more secure and convenient. By doing so, we are further protecting our mission-critical systems and data, which is critical to helping us protect the American consumer.

MFA Options

When accessing the Collect website, after entering your username and password, you need to select at least one of three CFPB-supported second authentication methods:

1. Salesforce Authenticator Mobile App

The Collect website is powered by Salesforce. The Salesforce Authenticator mobile app is integrated with the login process, is simple to install, and connects to your Collect account. Once set up, you will receive a push notification to your mobile device that can be used to approve the secondary authorization request to login. As needed, the Salesforce Authenticator mobile app can generate a six-digit code that users can enter on the second challenge screen with or without a cellular or wi-fi connection.

You can download the Salesforce Authenticator mobile app from the Google Play or Apple App Store.

2. Non-Salesforce (3rd Party) Authenticator Application (e.g., Google, Apple, Microsoft, Okta, or other desktop TOTP authenticators)

Salesforce also supports a wide variety of 3rd party verification applications that are simple to install on multiple operating systems and do not require connectivity. Like the Salesforce Authenticator application, the 3rd party application generates unique, temporary verification codes, and they can connect to your Collect accounts.

You can download the 3rd party authenticator mobile apps from the Google Play or Apple App Store or desktop applications from the Microsoft Windows or Apple (IOS) stores.

3. Hardware Security Device (e.g., Yubikey)

Hardware security devices, also known as security keys, are physical devices that connect to a user's computer and use public-key cryptography. Security keys are easy to use as they do not require any installation or manual entry of any codes. By pressing

the key's button(s), the device automatically generates and enters a code into the second challenge screen. Security keys are a good option if you do not have a mobile device near upon login or if you cannot download apps.

NOTE: CFPB is not responsible for providing any physical device to use this type of MFA. If you wish to use this option, follow the known channels through your IT department to request an approved device.

MFA Use, Considerations, and Additional Guidance

Before proceeding with MFA registration, please follow the guidance of your organization's Cyber Security for installing one of these supported MFA methods. It is recommended that the organization use their current/existing MFA app/key as the first option.

NOTE: Though not often, web compatibility issues sometimes occur with MFA. If you do experience MFA verification issues, please verify that you are not using an outdated web browser. This can cause issues when using MFA because an outdated browser may not support the latest security protocols or may have known vulnerabilities that can be exploited by hackers.

Additionally, the plugs-ins or extensions that you have installed in your browser, or browser settings set forth for your browser by your organization, may disrupt the verification process.

To avoid web compatibility issues with MFA, we encourage Collect users to:

1. Use the most recent version of the browser listed above and keep it up-to-date with the latest security patches and updates;
2. Clear or reset cookies and cache data from previous activities; and

- Verify if the browser has enabled pop-up blockers by default and adjust settings accordingly. Some pop-up blockers may prevent MFA prompts from appearing.

Steps to Access Collect Using the Salesforce Authenticator App

Step 1: Install the Salesforce Authenticator Mobile App

If you do not have the Salesforce Authenticator application already installed on your device, visit the Google Play or Apple App Store to locate and install the Salesforce Authenticator application. Please follow the prompts to install.

Step 2: Access the Collect Website

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Collect website at

<https://collect.consumerfinance.gov>.

Step 3: Login with Existing Collect Username and Password

Enter your existing '**Username**' and '**Password**' into the login screen. Ensure the username ends in ".cfpbportal."

This website is optimized for the following browsers: Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari.

cfpb Consumer Financial Protection Bureau

Welcome to Collect

Collect is the Bureau's online channel for financial institutions to submit credit card agreements, prepaid account agreements, college credit card marketing agreements, and the Terms of Credit Card Plans (TCCP) Survey. You cannot submit a complaint, respond to a complaint, submit HMDA data, or access any other Bureau collections through this website.

Ensure the username ends in ".cfpbportal".

Username: example@example.com.cfpbportal

Password

Log In

Need to set your password or Forgot your password?

If you have forgotten the Password, use the '**'Forgot Your Password'** link below the '**'Login'** button.

Step 4: Choose the Salesforce Authenticator Verification Method

On the '**'Choose a Verification Method'** screen, select the '**'Use the Salesforce Authenticator mobile app'** option.

salesforce

Choose a Verification Method

How would you like to verify your identity?

Use the Salesforce Authenticator mobile app

Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) key

Use verification codes from an authenticator app

Continue

Step 5: Connect the Salesforce Authenticator Mobile App

When users first access Collect and set up MFA using the Salesforce Authenticator mobile app, they must connect the app to their account. This only needs to be completed once.

Once on the '**Connect Salesforce Authenticator**' screen, open the Salesforce Authenticator mobile app and select the '**Add an Account**' button at the bottom. Obtain the two-word phrase provided and enter it into the '**Two-Word Phrase**' field. When finished, select the '**Connect**' button.

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the [App Store](#) or [Google Play](#) and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase

Cancel Connect

[Choose Another Verification Method](#)

Step 6: Verify Your Identity

On the '**Verify Your Identity**' screen, enter the six-digit code provided by the Salesforce Authenticator mobile app into the '**Verification Code**' field and then select the '**Verify**' button. The six-digit code refreshes every sixty seconds.

You're trying to Log In to CFPB Collect. To make sure your Salesforce account is secure, we have to verify your identity.

Use the authenticator app on your mobile device to generate a verification code.

Username: robert.collecttestduke@cfpb.gov.cfpbportal

Verification Code

Verify

If the code is correct, you will be directed to the Collect website homepage and can proceed as usual.

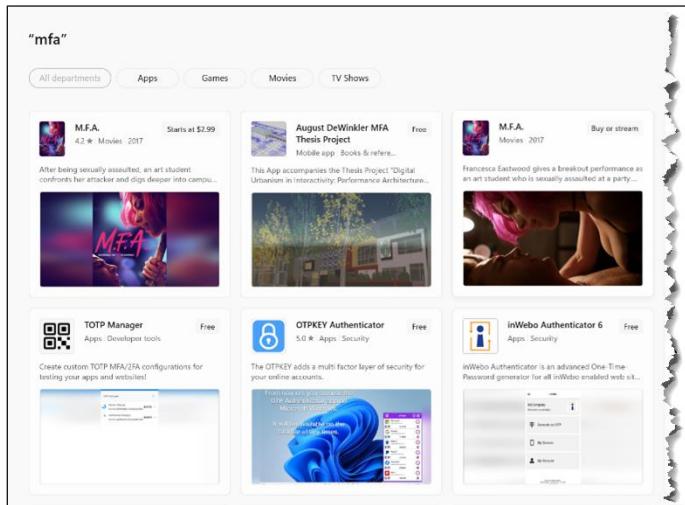
Steps to Access Collect Using the Using the Windows/Apple (iOS) Desktop Application for MFA

Note: These instructions will follow the installation and use of a Windows MFA application, however the process to install an Apple (iOS) MFA application follows the same basic steps but begins with accessing the Apple store to locate an iOS desktop MFA application.

Step 1: Install a Windows Desktop MFA Application

If you do not have a Windows Desktop MFA application already installed on your desktop/laptop, visit the Microsoft Store and type in “MFA” in the Search box and select the Enter key.

The Microsoft Store will display a range of MFA apps to select (see below). Select the application that your organization’s Cyber Security has approved. *Note: For these instructions, “TOTP Manager” will be used as an example.*



Select the **TOTP Manager** Authenticator and select the **Get** or download button. Follow the prompts to install.

A screenshot of the Microsoft Store product page for the "TOTP Manager" app by Toby Smith. The page includes a QR code, a screenshot of the app interface showing configuration options like "Days" and "Time Period", and a "Screenshots" section with a preview of the app's user interface. A red box highlights the "Get" button. Below the button, a note says "This app requires the latest version of Microsoft Edge." The app has 0 ratings. The description section states: "Create custom TOTP MFA/2FA configurations for testing your apps and websites! Create and store any number of TOTP configurations. Pick from multiple timespans ranging from 15 seconds to 10 minutes. Multiple hashing algorithms are supported including SHA-1 and SHA-256. See a whole range of codes including 5 into the past and 5 into the future! Also available as a website at https://totp-online.tobythe.dev". The "Ratings and reviews" section notes "There aren't any reviews for this product yet." The "Features" section lists "Create custom TOTP configurations", "See codes in the past and future", and "Use many different intervals and hashing algorithms".

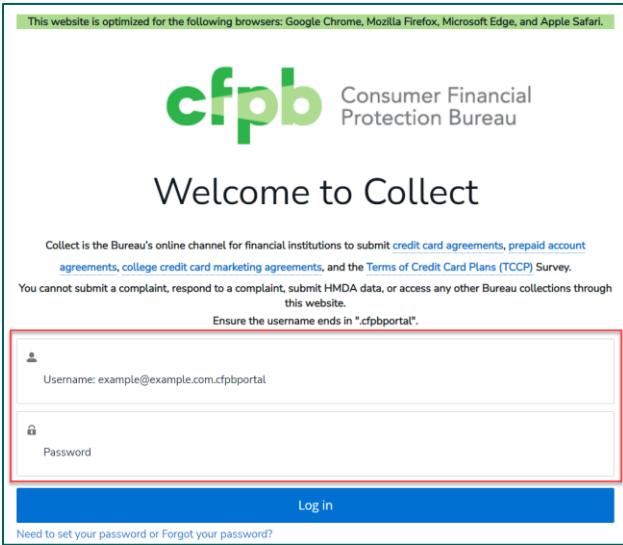
Step 2: Access the Collect Website

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Collect website at <https://collect.consumerfinance.gov>.

Step 3: Login with Existing Collect Username and Password

Enter your existing **'Username'** and **'Password'** into the login screen. Ensure the username ends in **".cfpbportal."**

This website is optimized for the following browsers: Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari.



cfpb Consumer Financial Protection Bureau

Welcome to Collect

Collect is the Bureau's online channel for financial institutions to submit credit card agreements, prepaid account agreements, college credit card marketing agreements, and the Terms of Credit Card Plans (TCCP) Survey. You cannot submit a complaint, respond to a complaint, submit HMDA data, or access any other Bureau collections through this website. Ensure the username ends in ".cfpbportal".

Username: example@example.com.cfpbportal

Password

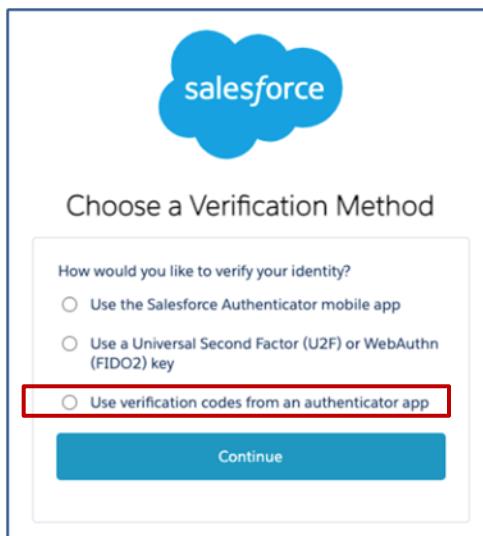
Log In

Need to set your password or Forgot your password?

If you have forgotten the Password, use the '**'Forgot Your Password'** link below the '**'Login'** button.

Step 4: Choose the Windows MFA Verification Method

On the '**'Choose a Verification Method'** screen, select the '**'Use verification codes from an authenticator app'** option.



salesforce

Choose a Verification Method

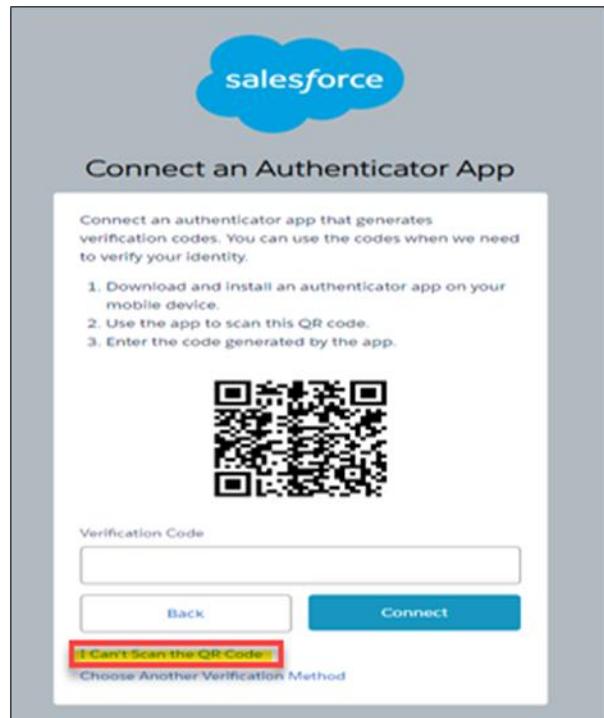
How would you like to verify your identity?

- Use the Salesforce Authenticator mobile app
- Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) key
- Use verification codes from an authenticator app

Continue

Step 5: Connect an Authenticator App

When the **'Connect an Authenticator App'** screen appears, select **I Can't Scan the QR Code**.



salesforce

Connect an Authenticator App

Connect an authenticator app that generates verification codes. You can use the codes when we need to verify your identity.

1. Download and install an authenticator app on your mobile device.
2. Use the app to scan this QR code.
3. Enter the code generated by the app.



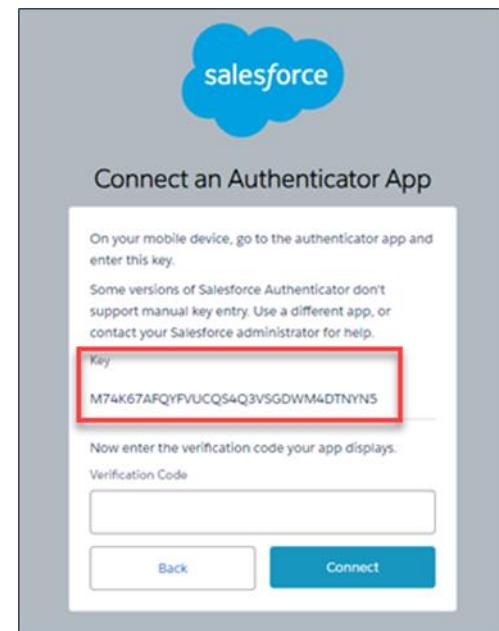
Verification Code

Back **Connect**

I Can't Scan the QR Code

Choose Another Verification Method

A numeric key will be generated in the **Key** section. Copy this key to be used in a later step.



salesforce

Connect an Authenticator App

On your mobile device, go to the authenticator app and enter this key.

Some versions of Salesforce Authenticator don't support manual key entry. Use a different app, or contact your Salesforce administrator for help.

Key

M74K67AFQYFUCQS4Q3VSGDW4DTNYNS

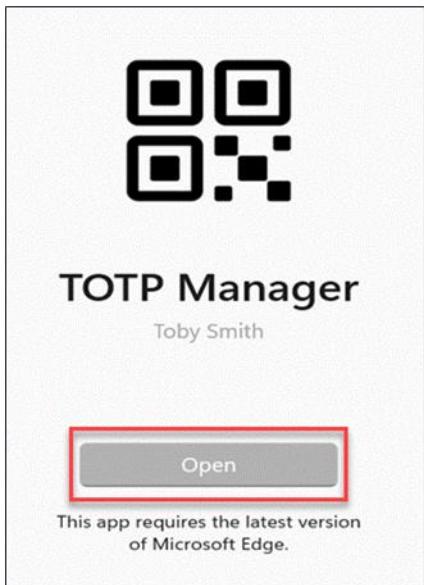
Now enter the verification code your app displays.

Verification Code

Back **Connect**

Step 6: Complete Authenticator App Verification

Return to the installed Authenticator application, e.g., TOTP Manager, and follow the prompts.



Add a new TOTP < Back

About

Account	Issuer (Optional)
Collect	SF Test

Configuration

Secret	Generate
M74K67AFQYFVUCQS4Q3VSGDWM4DTN	

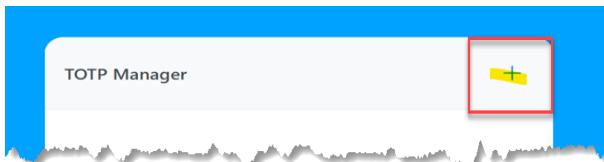
Digits	Time Period	Algorithm
6	30 seco...	SHA-1

Create!

A six-digit code will be created, e.g., **404140**. Copy the number.

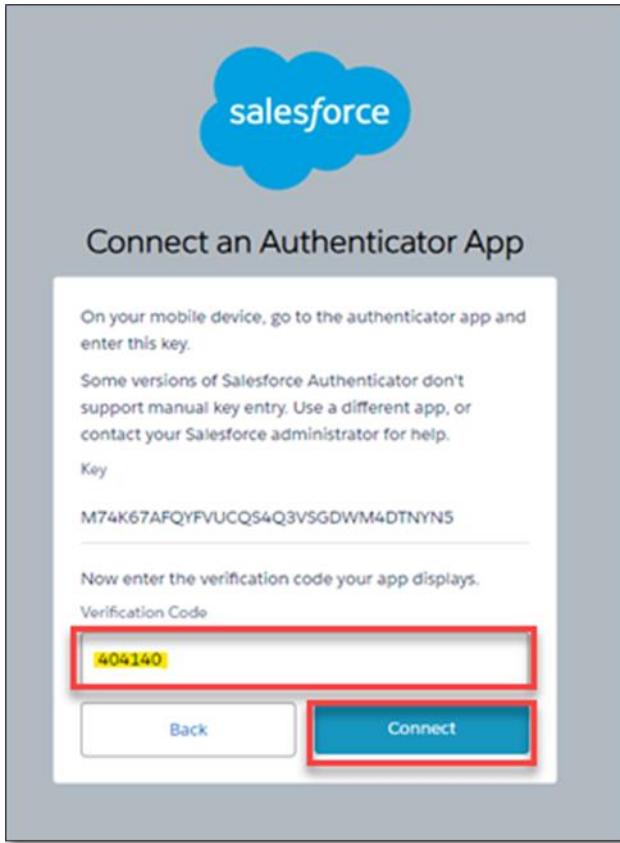


Select the **+** sign to add a credential.



On the next screen, enter **Collect** into the **Account** field. Paste the **Key** copied at the end of Step 5 into the **Secret** field and select **Create**.

Return to the **Connect an Authenticator App** screen, enter or paste from your clipboard the six-digit code in to the **Verification Code** box and select **Connect**.



This should complete your MFA authentication process.

Note: Salesforce may ask that you re-login and enter the MFA code during the log-in process.

Steps to Access Collect Using a Universal Second Factor (U2F) or WebAuthn (FIDO2) Key (e.g., a YubiKey) for MFA

If you wish to use this option, follow the known channels through your IT department to request an approved device. Once approved and received, follow the steps below or as designated by your IT department. The following steps describe the use of

a YubiKey device, but other approved devices follow similar steps.

Step 1: Access the Collect Website

Using a compatible browser (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), access the Collect website at <https://collect.consumerfinance.gov>.

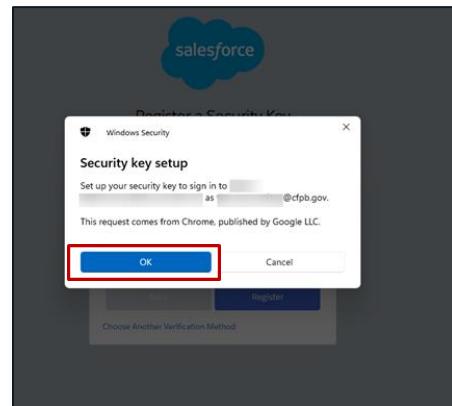
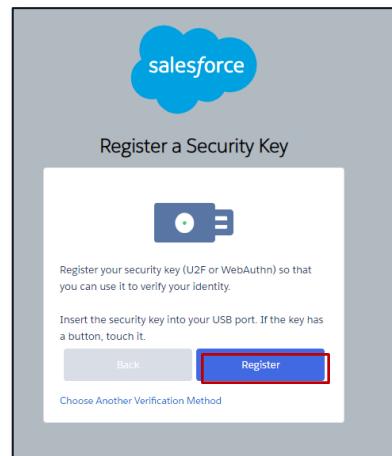
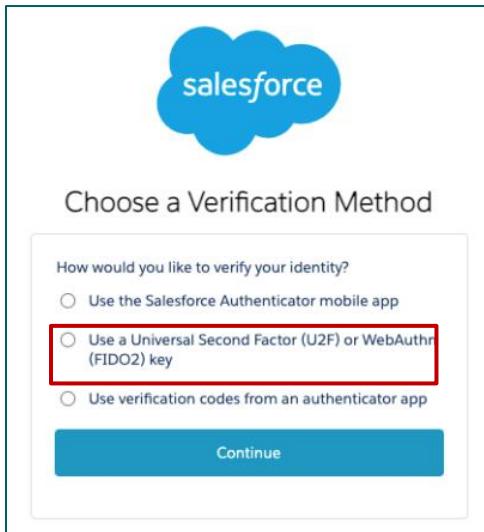
Step 2: Login with Existing Collect Username and Password

Enter your existing '**Username**' and '**Password**' into the login screen. Ensure the username ends in '.cfpbportal.'

If you have forgotten the Password, use the '**Forgot Your Password**' link below the '**Login**' button.

Step 3: Choose the Universal Second Factor (U2F) or WebAuthn (FIDO2) key method (specifically the use of a YubiKey)

On the Choose a Verification Method screen, select the **Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) Key** option. You will be directed to the Register a Security Key screen.

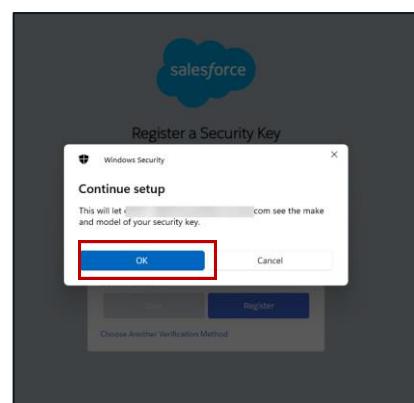


Step 3: Register and Set Up Your Security Key

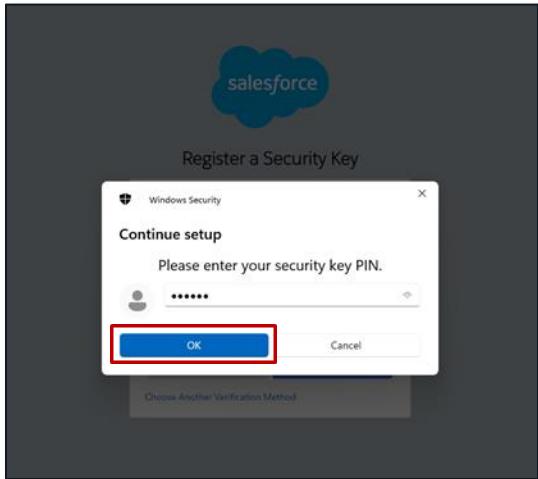
On the **Register a Security Key** screen Follow the instructions, insert your security key into a USB port, touch a button (if it has one), and then select **Register**.

The **Security key setup** screen will appear, with text that advises you are setting up the key to sign-in to the Collect URL with your designated username. Select **OK**.

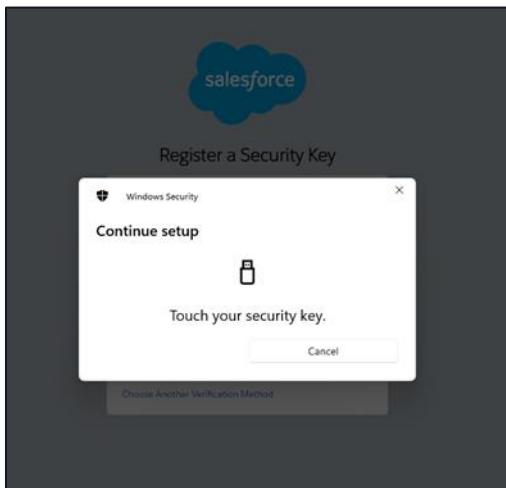
On the **Continue setup** screen, a confirmation of your security key (i.e., YubiKey) allowing the Collect website to see your security key. Select **OK**.



On the next **Continue setup** screen, enter the security key PIN that you created when you obtained your key (i.e., YubiKey). Select **OK**. Note: *The PIN would have been setup by you when you obtained it; contact your IT department if you have any issues*

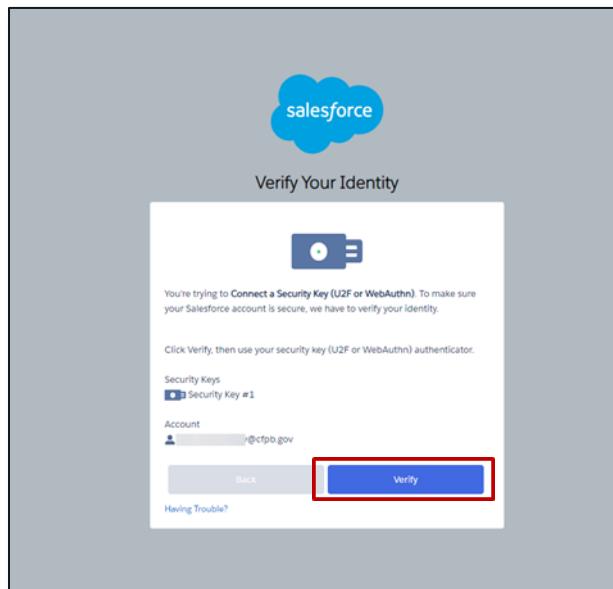


On the next **Continue setup** screen, follow the instructions to “**Touch your security key**”.

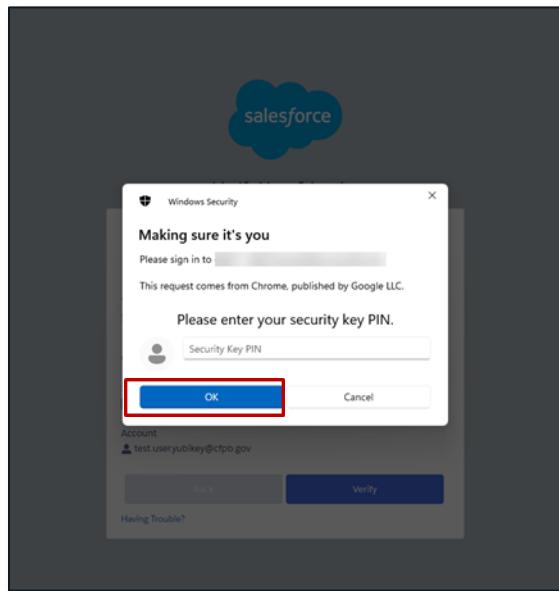


Step 4: Verify Your Identity (with your Security Key, e.g., YubiKey)

The **Verify Your Identity** screen will appear after touching your security key in the previous step. This series of steps verifies you and the security key for future logins. Verify the information presented and select **Verify**.



On the **Making sure it's you** screen, re-enter your security key pin. Click **OK**. Note: *Like Step 3 above, the PIN would have been setup by you when you obtained your security key; contact your IT department if you have any issues.*



Step 5: Next and Subsequent Logins to the Collect Website

Upon the next login, and any future logins, to the Collect website (<https://collect.consumerfinance.gov>) enter your username and password; you will be prompted to use your security key. Touch the security key, e.g., YubiKey, and you will immediately be logged in.

Collect Support

If you have any questions regarding MFA or experience any issues, please send us an email, detailing the MFA issue in the subject line at

Collect_Support@cfpb.gov