FTC Administrative E-Filing System

External User Registration Guide

(Filer)

October 2025

Table of Contents

1. Introduction 3
2. Overview 3
3. Application/User Registration 3
3.1 New/First time Users 3
3.1.1 Registration 3
3.1.2 Account Activation 6
3.1.3 Setup Multi-Factor Authentication 8
3.1.4 Updating Multi-Factor Authentication Settings 27
3.2 Registered Users 28
3.2.1 Login 28
3.2.2 Reactivate Account 32
4. Login to Administrative E-Filing 39
5. Troubleshooting 39

1. Introduction

The Federal Trade Commission's (FTC's) Administrative E-Filing System (AEFS) is a new web-based, user-friendly application that receives electronic filings in adjudicative proceedings conducted under Part 3 of the Commission's Rules of Practice that governs how competition and consumer protection cases are tried before an Administrative Law Judge (ALJ). The FTC's new Administrative E-Filing Application has been created to secure, streamline and improve efficiencies for FTC's Administrative E-Filing application users.

2. Overview

This Administrative E-Filing System (AEFS) User Guide is an instruction manual that provides guidance on how to navigate and securely access the Admin E-Filing System for an optimal user experience.

3. Application/User Registration

3.1 New/First time Users

3.1.1 Registration

In order to access the Administrative E-Filing System, you must first register and create an account.

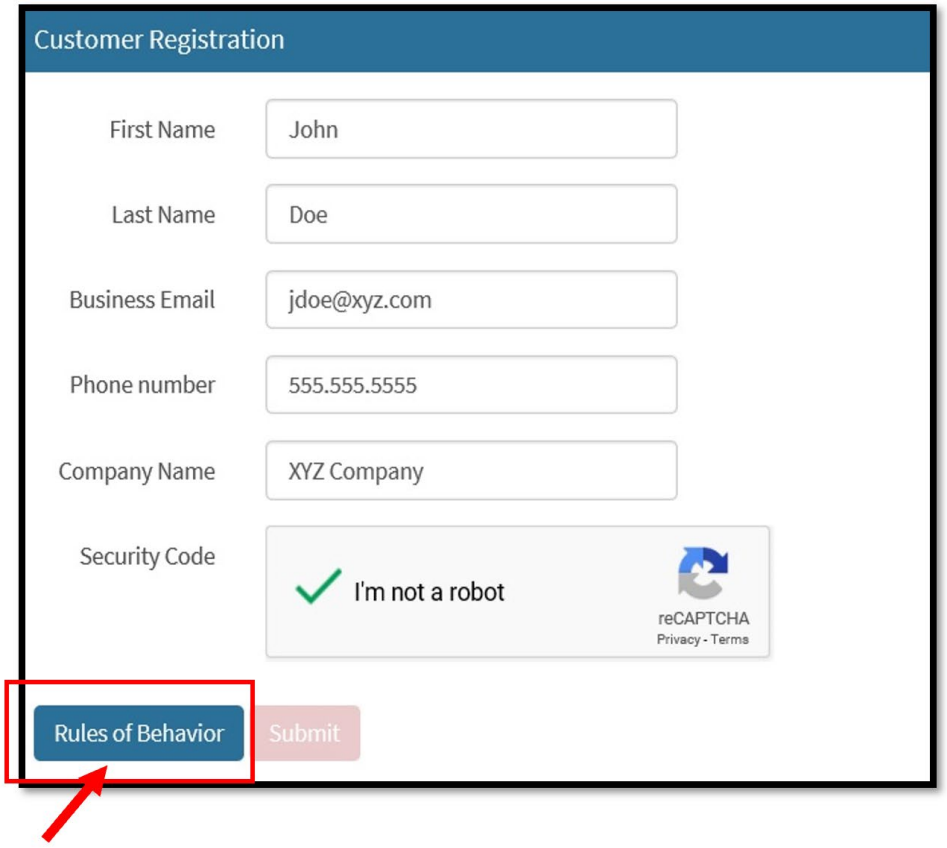
Please follow the steps below to register and create an account:

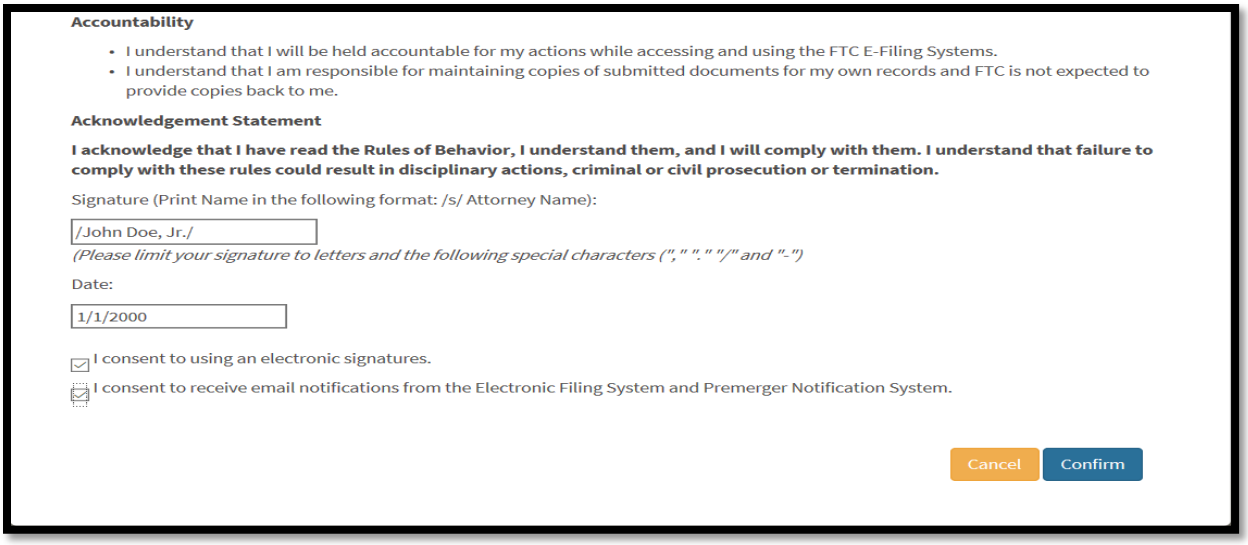
1) Click on the link below and then click on "*Register"* under *New Users:* **https://adminefiling.ftc.gov**

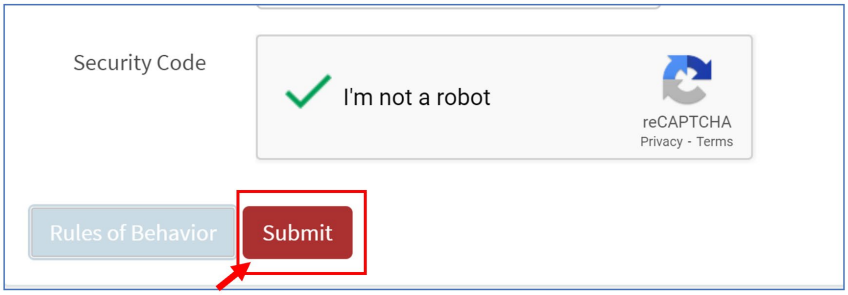
2) You will be redirected to the Customer Registration Page. To successfully complete registration, you must:

- First, enter in the requested information for each of the input fields on the Customer Registration page
- Then, click on the "**Rules of Behavior"** button and review the Rules thoroughly.
- After you have reviewed the rules, you must sign and date the Rules of Behavior. *Note: You must input the signature in the following format: "/name of the user/".*
- Next, enter in the Security Code (reCAPTCHA)
- Finally, click on "Submit" to complete the registration process

***PLEASE NOTE*: All users MUST sign the Rules of Behavior to complete the registration process.**

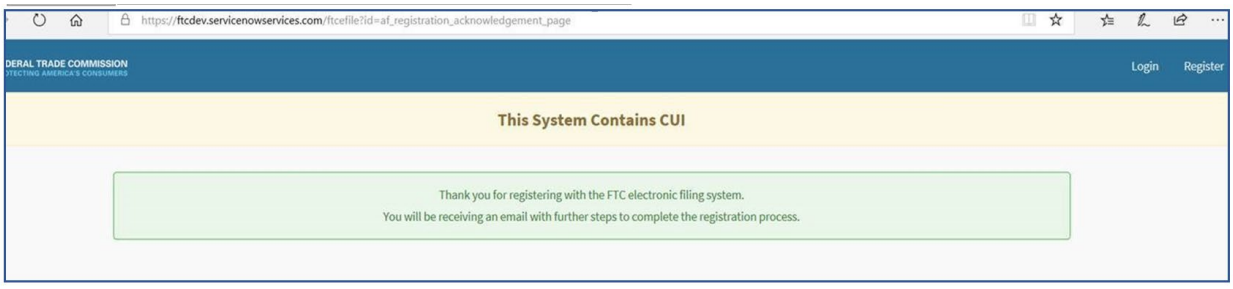






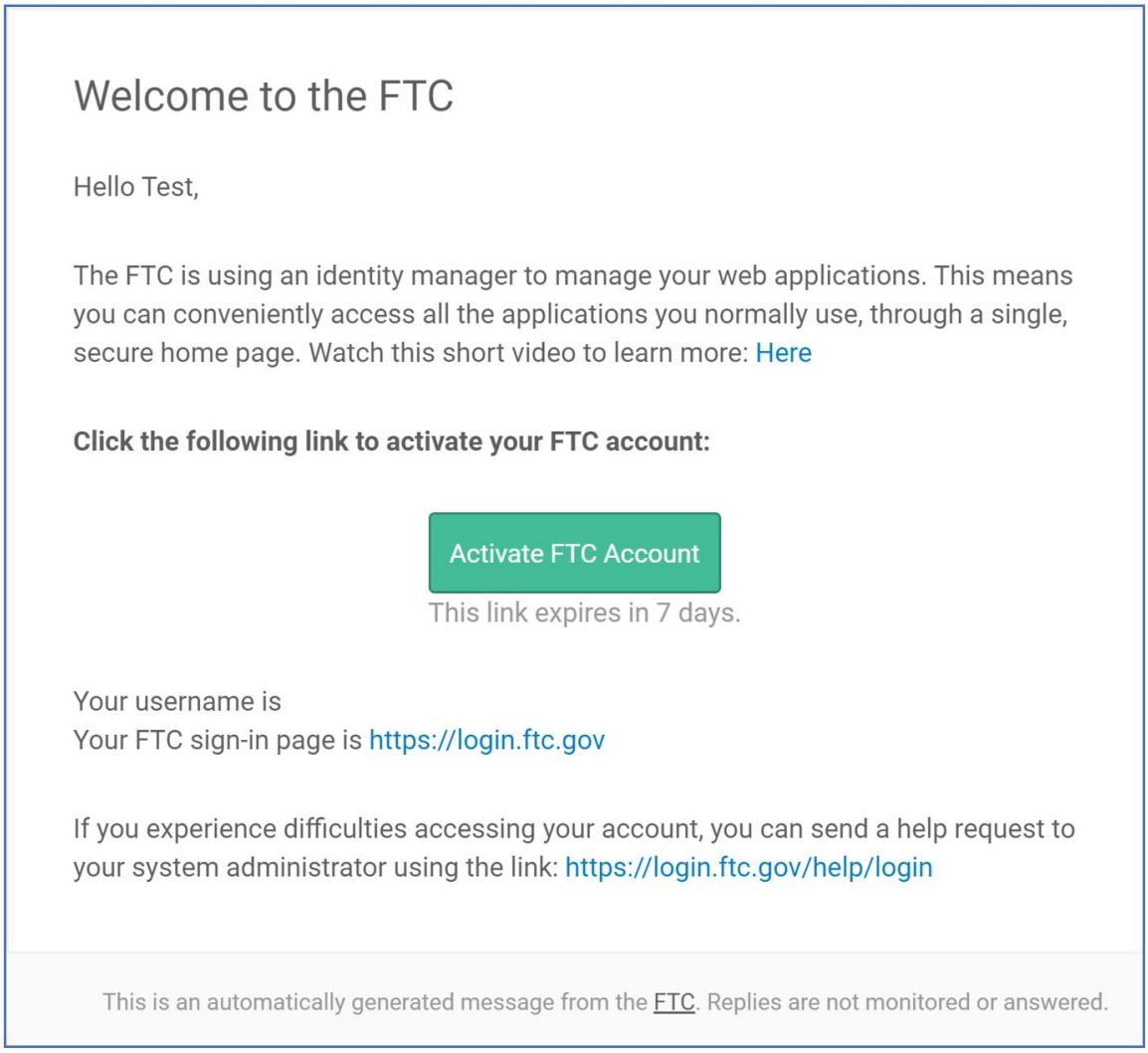
The Submit button will now be enabled and you can click on it to proceed.

3) Upon successful submission, the application will display a confirmation page, and you will receive an email with next steps to "Activate" your account with the FTC.



3.1.2 Account Activation

Upon receiving the activation email (example below) from the FTC, click on the "Activate FTC Account" button to activate your account.



Welcome to the FTC

Hello Test,

The FTC is using an identity manager to manage your web applications. This means you can conveniently access all the applications you normally use, through a single, secure home page. Watch this short video to learn more: Here

Click the following link to activate your FTC account:

Activate FTC Account

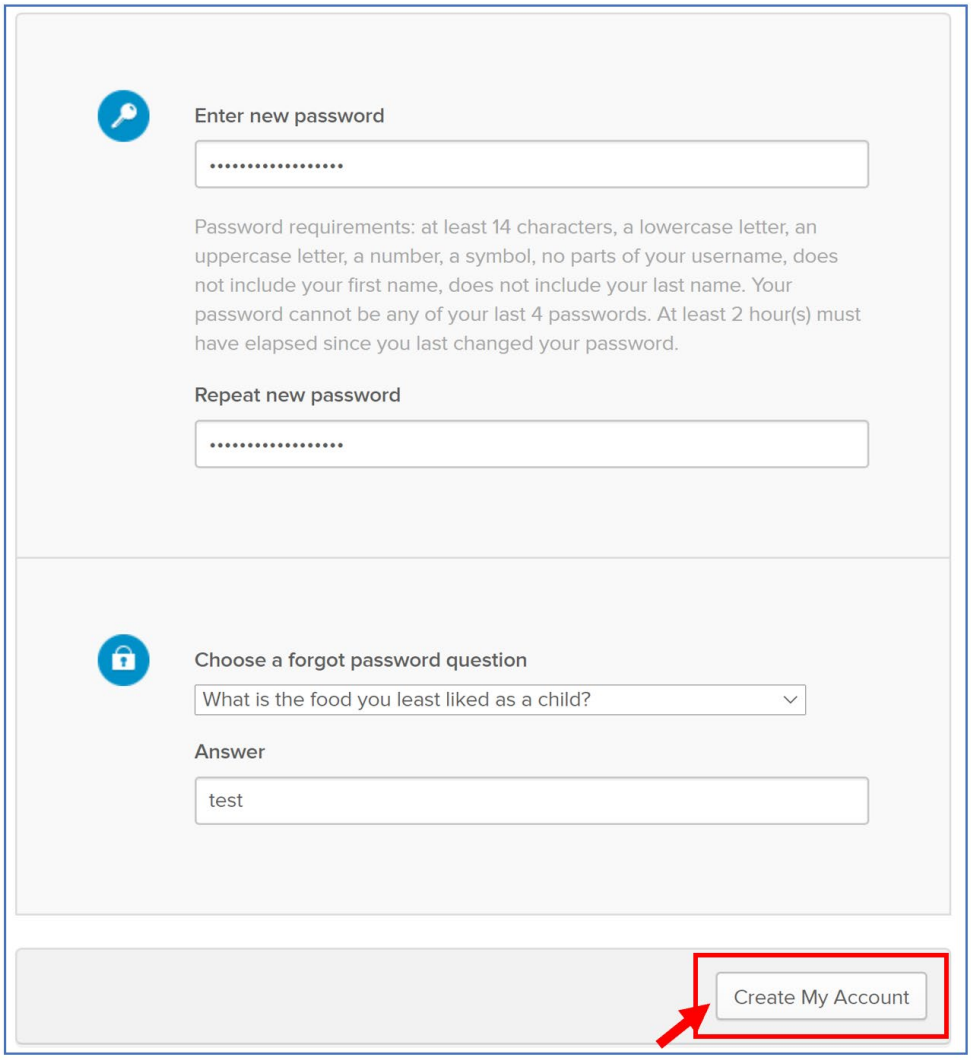
This link expires in 7 days.

Your username is
Your FTC sign-in page is https://login.ftc.gov

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link: https://login.ftc.gov/help/login

This is an automatically generated message from the FTC. Replies are not monitored or answered.

Upon clicking on the Activate link from your email, you will be automatically redirected to the FTC "Create your FTC account" page. Please enter in a new password, then repeat the password, then answer your security questions and click "Create Account".



3.1.3 Setup Multi-Factor Authentication

You will now need to set up your Multi-Factor Authentication (MFA); **You are only required to configure one (1) MFA factor**, however, multiple MFA options can be setup**:** Google Authenticator, Okta Verify – mobile, and/or Security Key or Biometric Authenticator, also known as FIDO2 (WebAuthn). We suggest that you complete this portion on a desktop or laptop because you will need to scan the QR code with your mobile device to complete.

Important Notice Regarding Security Key or Biometric Authenticator, FIDO2 (WebAuthn)

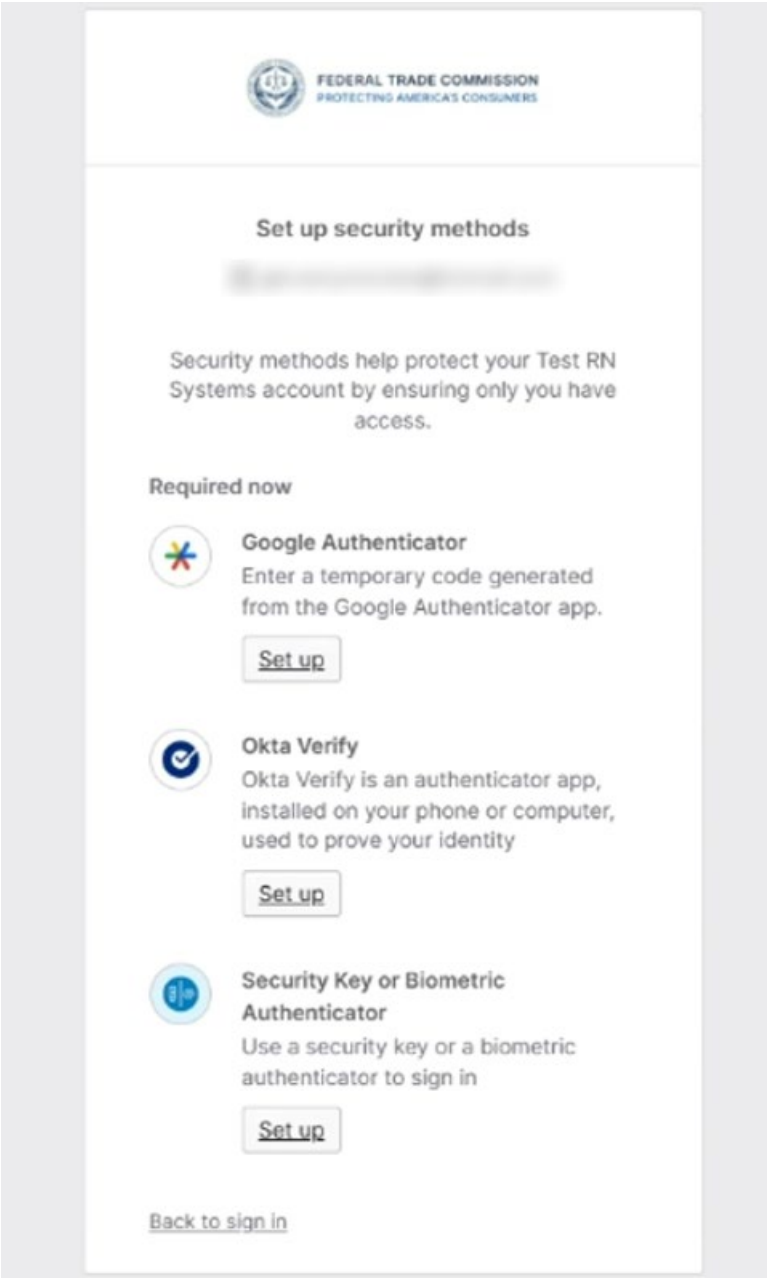
FIDO2 is the only phishing-resistant option. We suggest YubiKey 4 or higher. However, please be advised that the FTC **will not be able to provide support or resources for obtaining hardware tokens or other physical security keys or use of biometrics** for phishing-resistant MFA. While the FTC strongly encourages the use of phishing-resistant MFA to enhance security, individuals and organizations are responsible for acquiring and managing their own authentication hardware and ensuring devices are FIDO2 compliant.

FIDO2 Security Key Options:

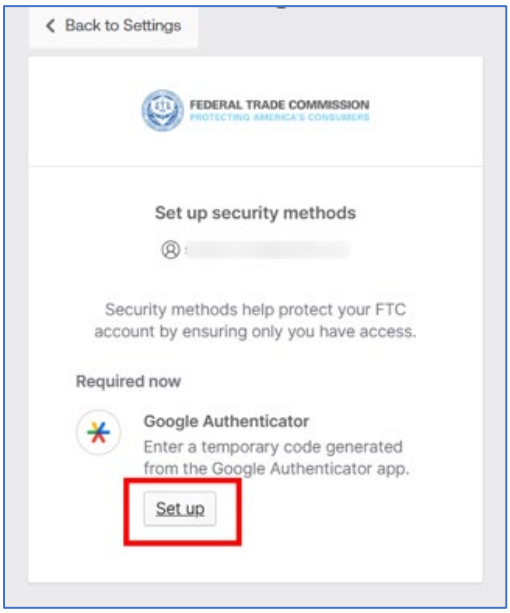
- **YubiKey** (suggested) – YubiKey 4 (2015) or higher
- **Google Titan Security Key** – USB-A and NFC; widely supported
- **Token2 T2F2 Series** – Affordable keys with USB-A, USB-C, and NFC options
- **Feitian BioPass Series** – Biometric security keys (fingerprint) with FIDO2 support
- **SoloKeys Solo V2** – Open-source USB-C or USB-A keys with FIDO2/WebAuthn

Note: If you are unable to setup or use your security key or biometrics, please select another MFA option. Okta Verify is the suggested method of authentication if not using FIDO2.

Please select your option and click “Setup”.

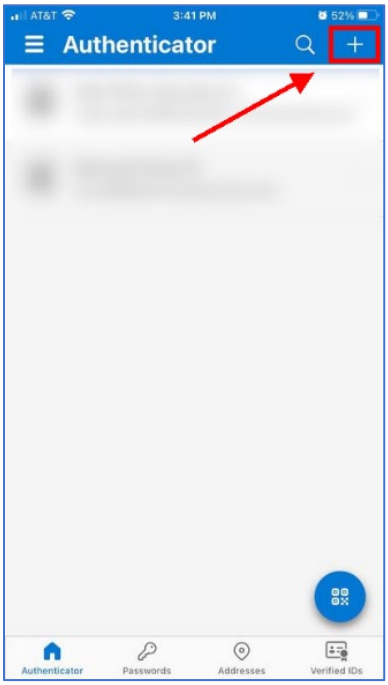


A. If you choose "Google Authenticator", **you will need to download the Google Authenticator App from the App Store on your mobile device to proceed via Google**.

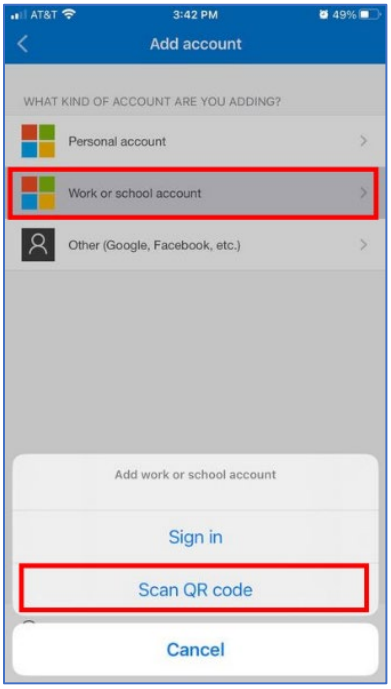


Continue by clicking "Set up".

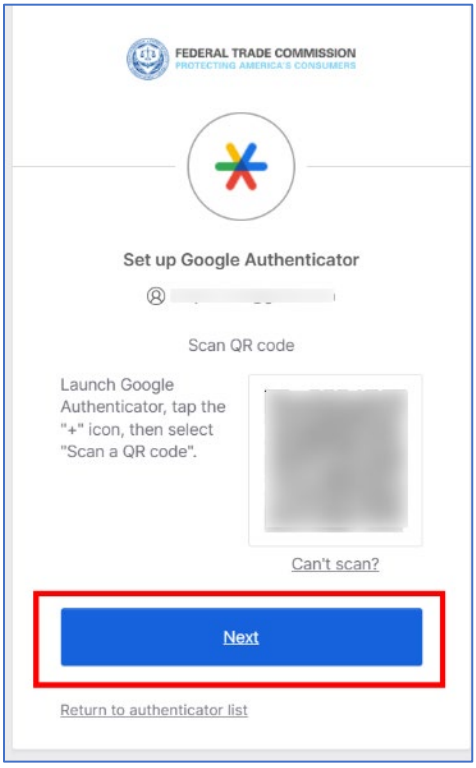
1. Open Google Authenticator app on your mobile device.
2. Select the "+".



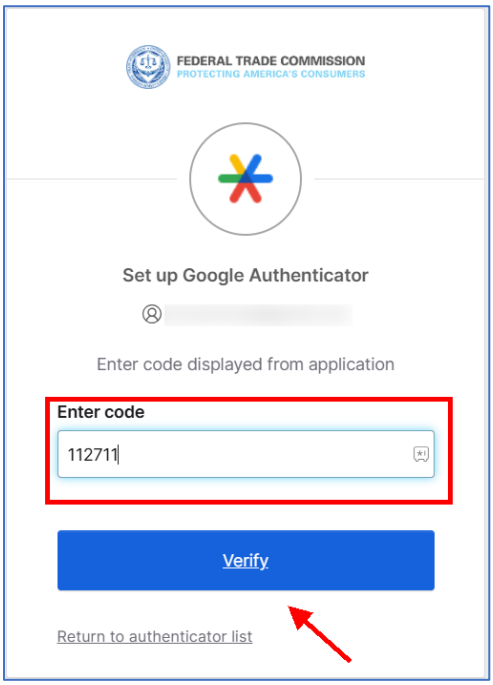
3. Select “Work or School Account” and “Scan QR code”.



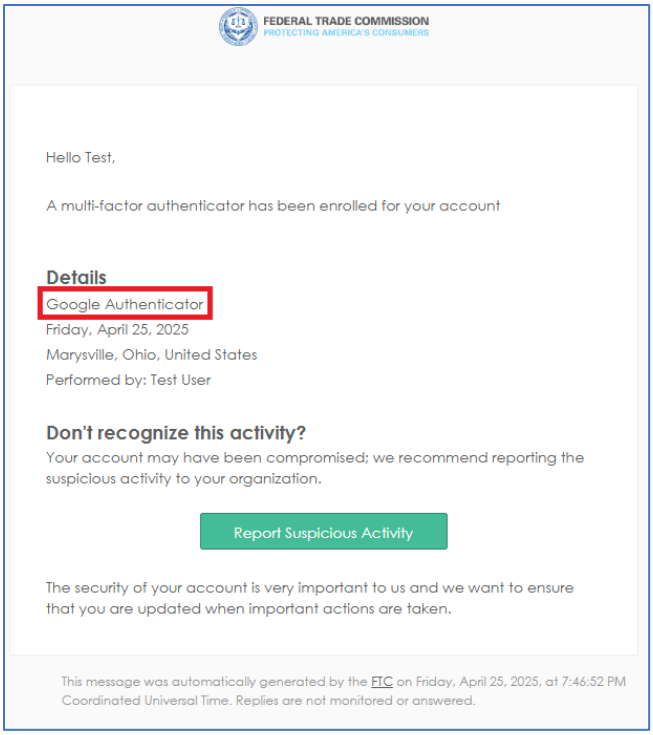
4. Your website page will display a QR code on your computer screen that you need to scan with the Google Authenticator app on your mobile device and click “Next”.



5. Once Google Authenticator is configured, you will be asked to verify by entering the rolling One Time Password (OTP). Enter OTP from your phone onto your computer screen and click “Verify”.



6. You will also receive an email confirmation with regarding your enrollment in “Google Authenticator” as shown below:

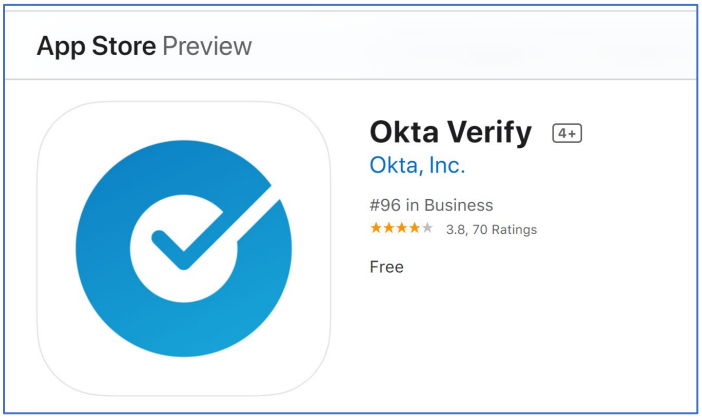


You have now successfully configured the Google Authenticator!

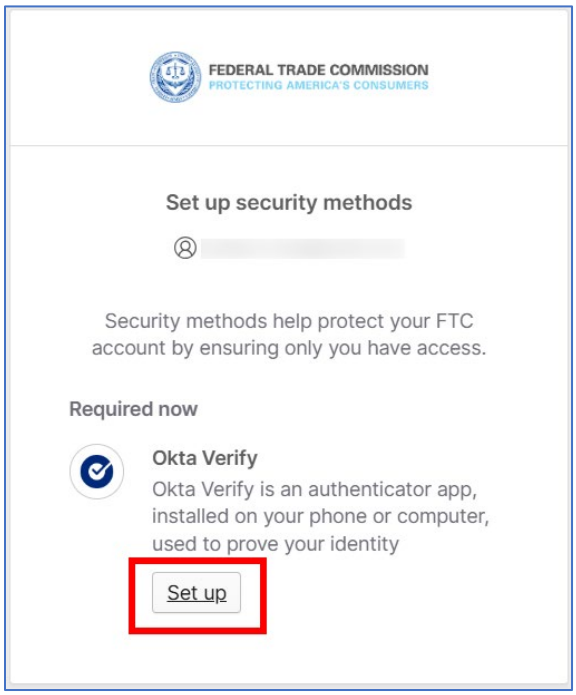
Your account registration with the FTC is now complete. You can now conveniently access all external FTC applications to which you have access through this account.

B. If you selected "Okta Verify", **<u>you will need to download the Okta Verify App from the App Store onto your mobile device to proceed via Okta.</u>**

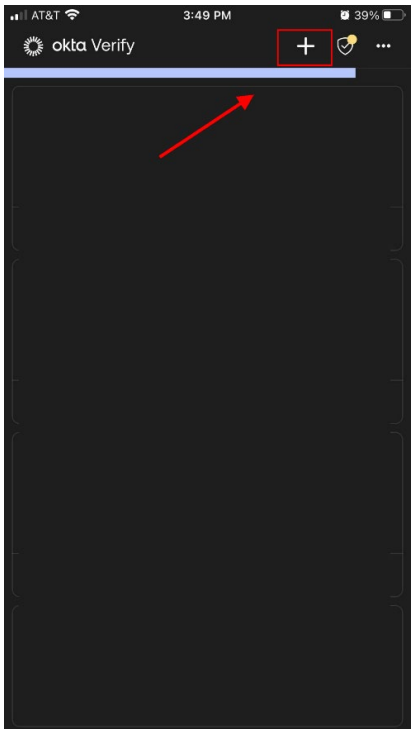
Please select your device type and click "Next".



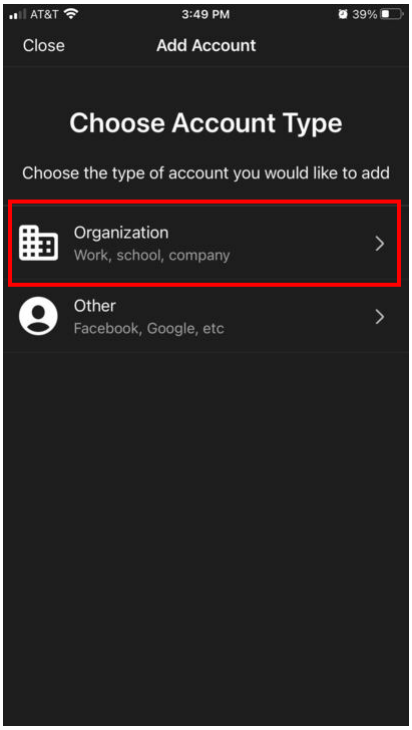
Continue by clicking “Set up” for Okta Verify.



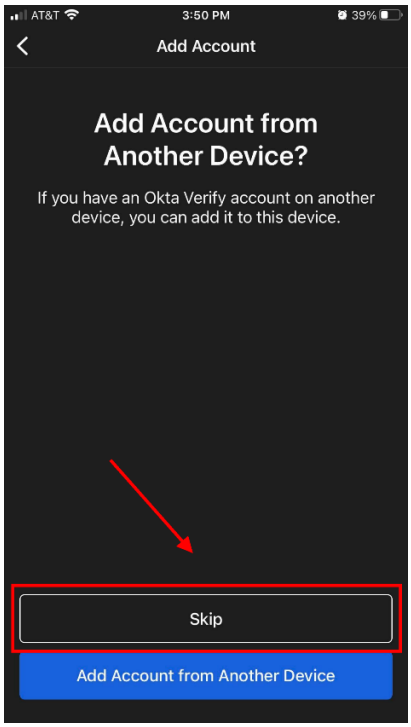
1. Open Okta Verity application on your mobile device. (Android/iPhone).
2. Select “+”.



3. Select Add “Work or School Account”.

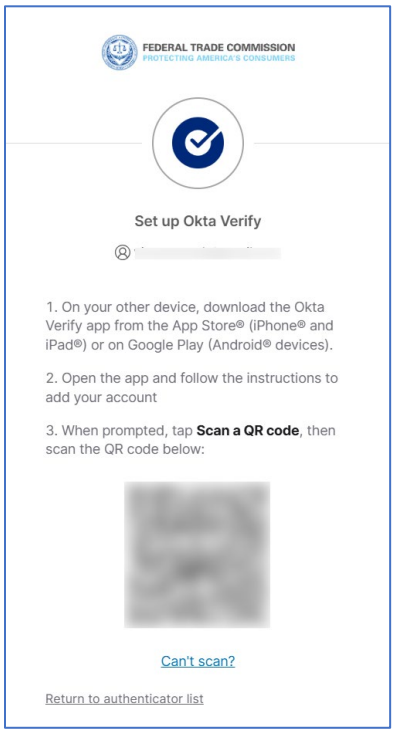


4. If you happen to have another Okta Verify account configured, you can press “Skip,” if not, then you can ignore this screen because the account you are setting up will become your default account.

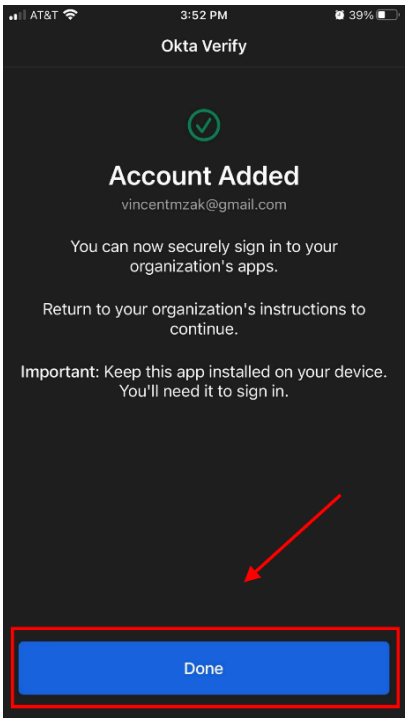


5. Select “Yes. Ready to Scan”.

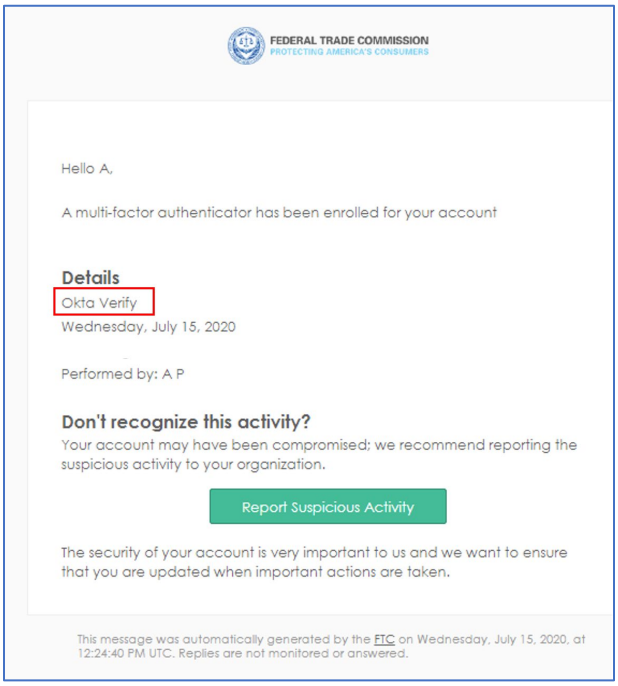
6. Okta will display a QR code on your computer screen that you will need to scan with the Okta Verify app on your mobile device.



7. Once the "Okta Verify" process is complete, you will see a green check mark against the Okta Verify enrollment as shown below. Now select "Done".



8. You will also receive an email confirmation with regarding your enrollment in "Okta Verify" as shown below:



You have now successfully configured the Okta Verify!

Your account registration with the FTC is now complete. You can now conveniently access all external FTC applications to which you have access through this account.

C. If you choose "Security Key or Biometric Authenticator" (also known as FIDO2 (Webauthn)), **you will need the Security Key hardware token on your person and available to insert into your device or have the biometric authentication already setup on your computer**.

If using Security Key enrollment:

- You must have a computer with a USB port.
- You must have a supported browser: Chrome, Firefox, Edge, or Safari.
- Your Security Key should be unlocked and ready.

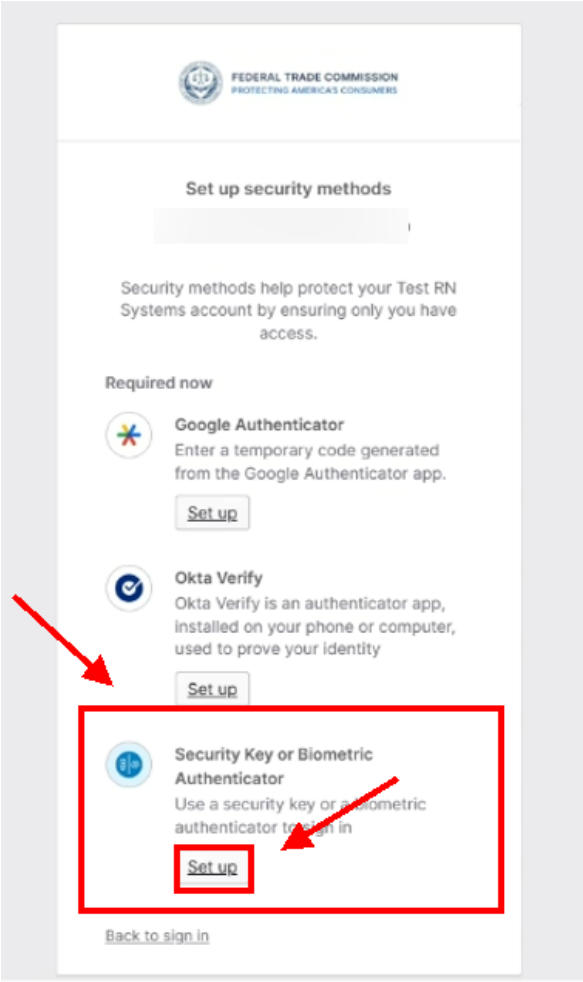
If using Biometric Authenticator enrollment, you will need to have already set it up on your computer based upon your computer's system requirements.

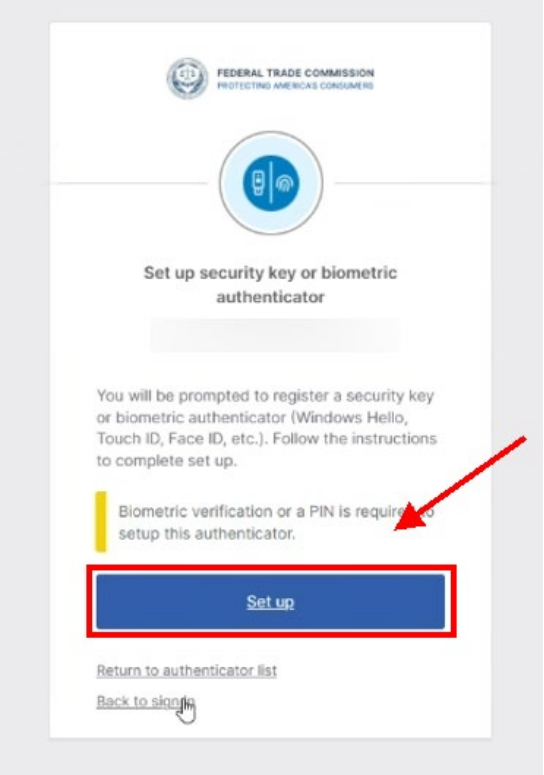
Note: If you are unable to setup or use your security key or biometrics, please select another MFA option.

The Security Key enrollment example below only mirrors YubiKey setup. If you chose a different FIDO2 hardware token or choose to use biometrics, please follow the steps Okta will provide on screen during your enrollment process.

Step 1: Enroll Your YubiKey as a Security Key

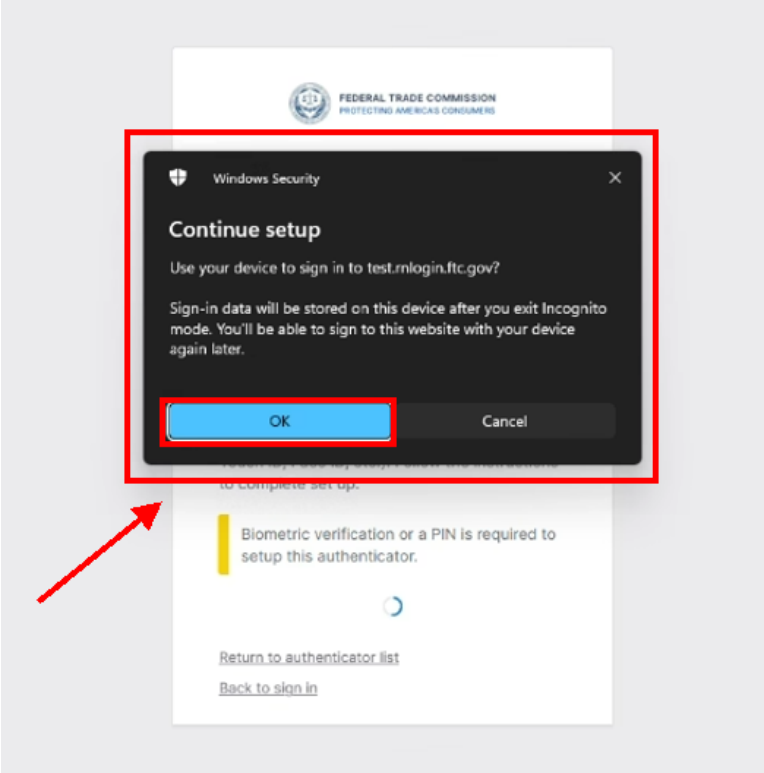
1. You must have a YubiKey 4 (2015) or higher.
2. Look for the option called "Security Key or Biometric Authenticator", also known as FIDO2 (WebAuthn).
3. Click "Set up".
4. A popup or new window will appear prompting you to begin registration.



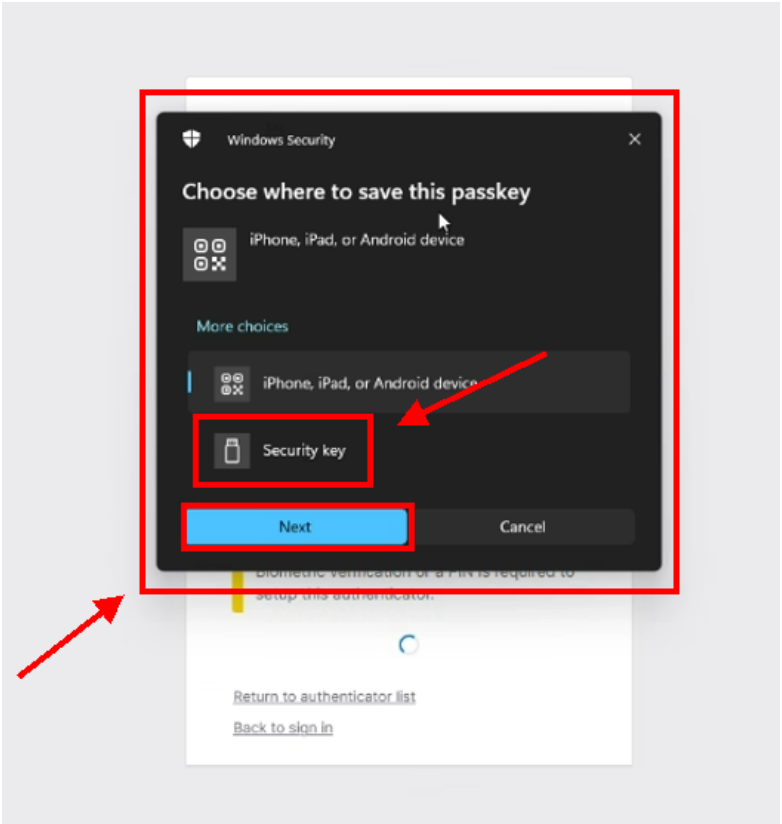


Step 2: Insert and Register Your YubiKey

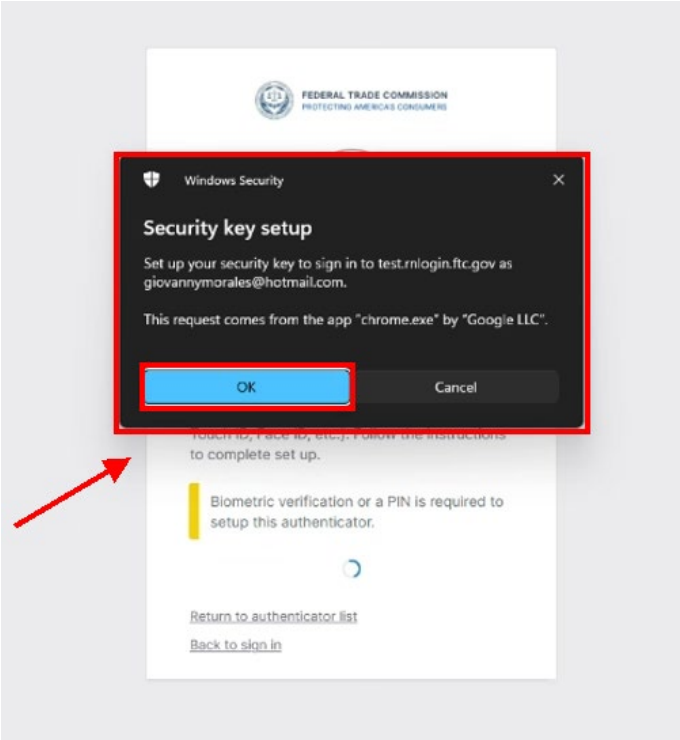
1. Insert your YubiKey into a USB port (or tap it to your device if using NFC).
2. Follow the browser prompt.
3. Touch the metal contact on your YubiKey when prompted.
4. Your browser and Okta will complete the registration.
5. You may be asked to give your key a nickname (e.g., “Work YubiKey”).
6. Select “OK”.



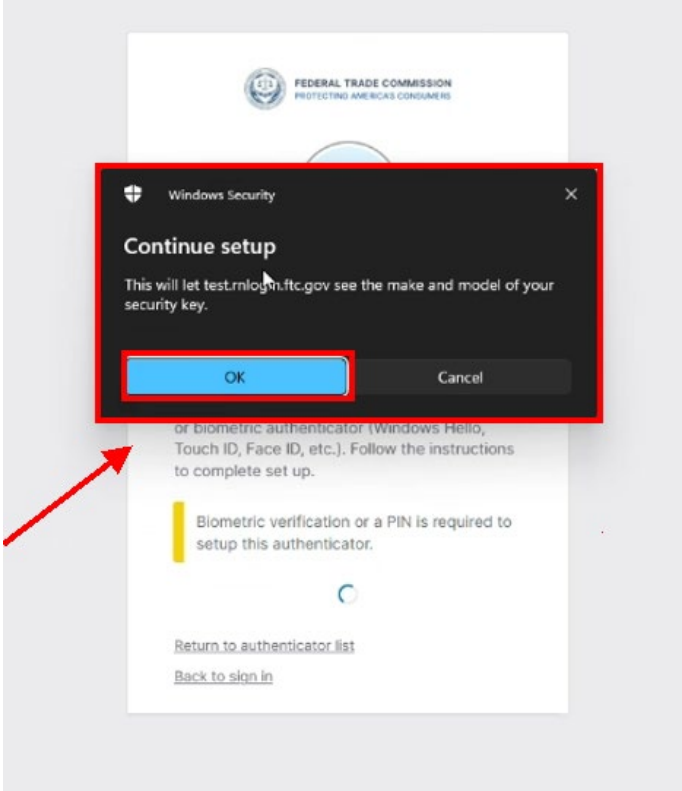
Click “OK” for the “Security Key Setup”.



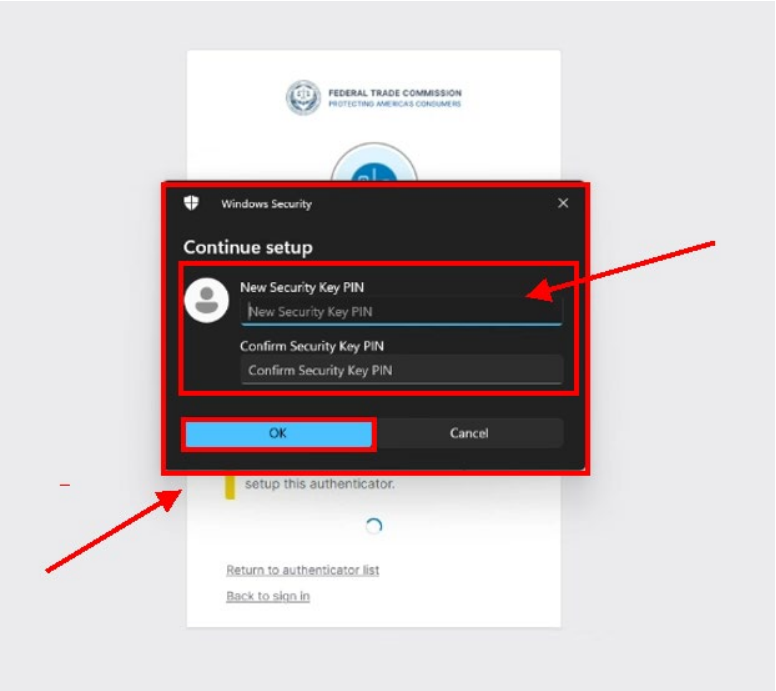
Click “OK”.



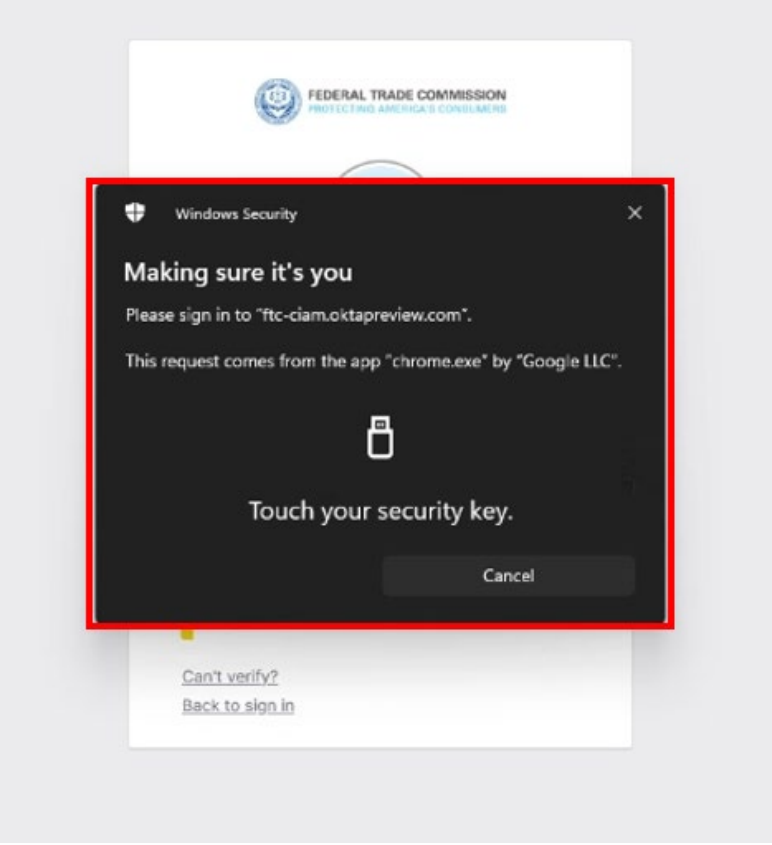
Click “OK” to Continue Setup.



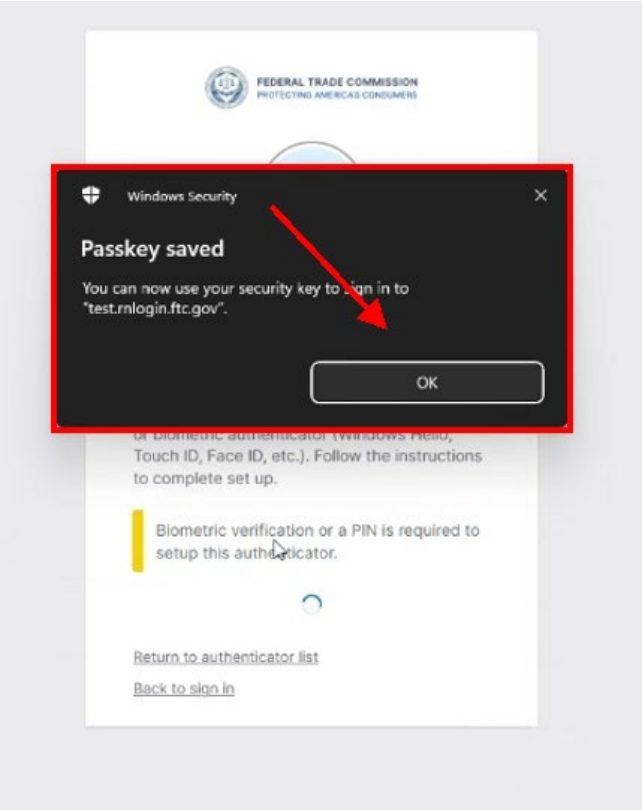
Enter a “PIN” and confirm the “PIN” number, select “OK”.



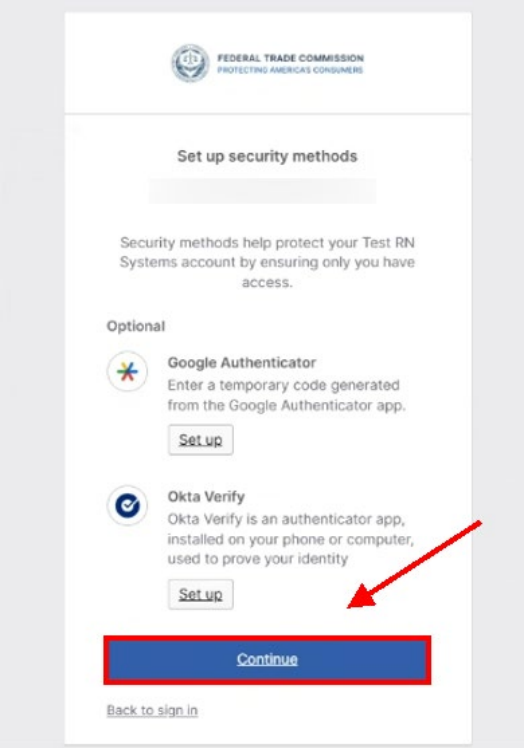
You will then be prompted to touch your “YubiKey”.

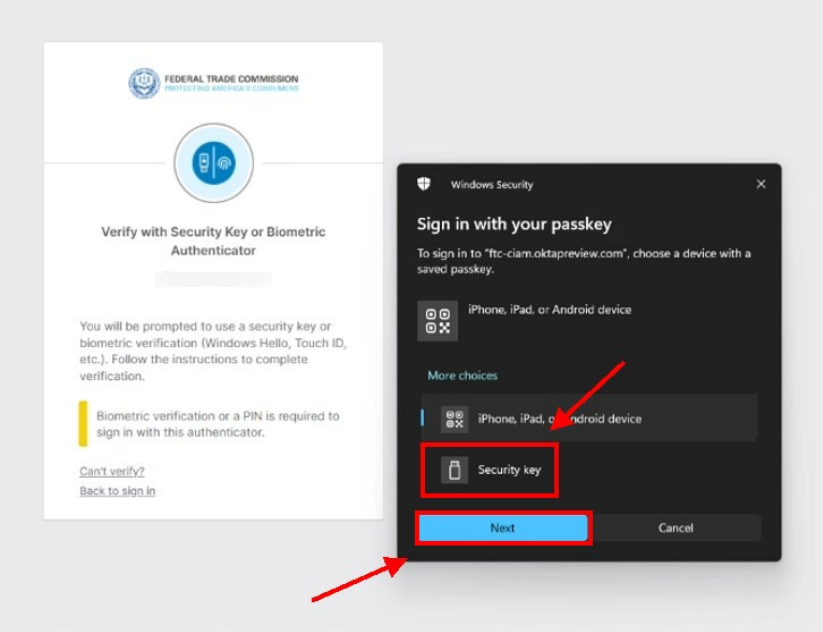


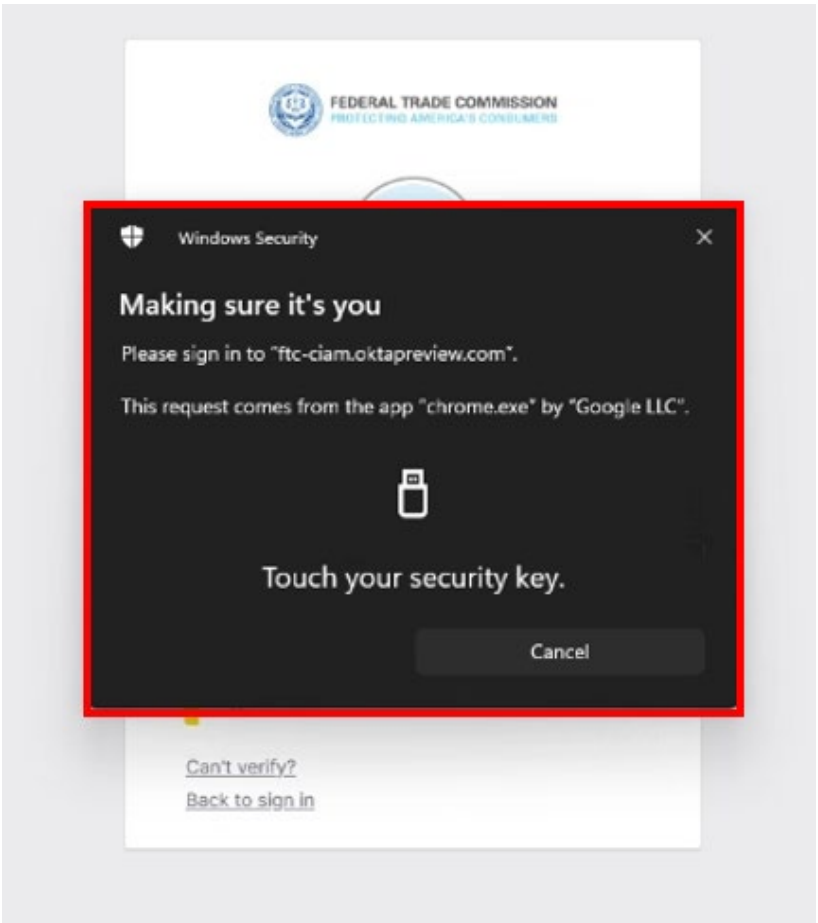
Your Passkey has now been saved, click “OK”.



Now select “Continue” or configure another MFA factor if you choose, but not required.

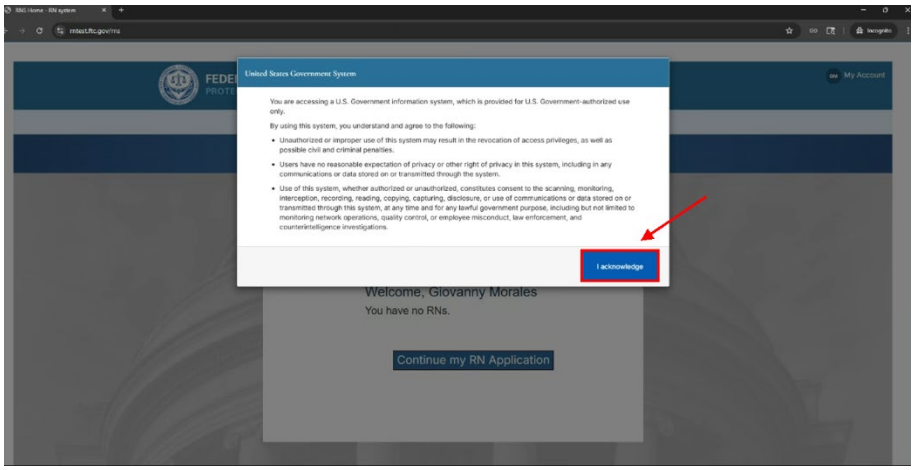



FEDERAL TRADE COMMISSION
Verify with Security Key or Biometric Authenticator
You will be prompted to use a security key or biometric verification (Windows Hello, Touch ID, etc.). Follow the instructions to complete verification.
Biometric verification or a PIN is required to sign in with this authenticator.
Can't verify?
Back to sign in
Windows Security
Sign in with your passkey
To sign in to "ftc-ciam.oktapreview.com", choose a device with a saved passkey.
iPhone, iPad, or Android device
More choices
Security key
Next
Cancel

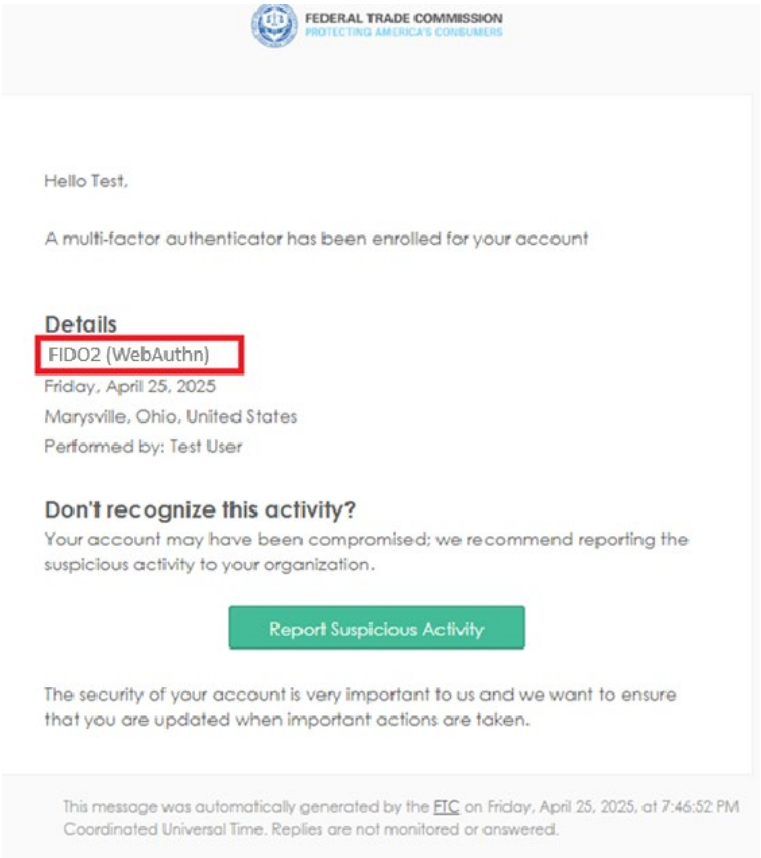

FEDERAL TRADE COMMISSION
Windows Security
Making sure it's you
Please sign in to "ftc-ciam.oktapreview.com".
This request comes from the app "chrome.exe" by "Google LLC".
Touch your security key.
Cancel
Can't verify?
Back to sign in

Step 3: Confirm and Save

1. Once successfully enrolled, Okta will display confirmation.
2. You can now use this YubiKey for authentication.



3. You will also receive an email confirmation with regarding your enrollment in "FIDO2 (WebAuthn)" as shown below:



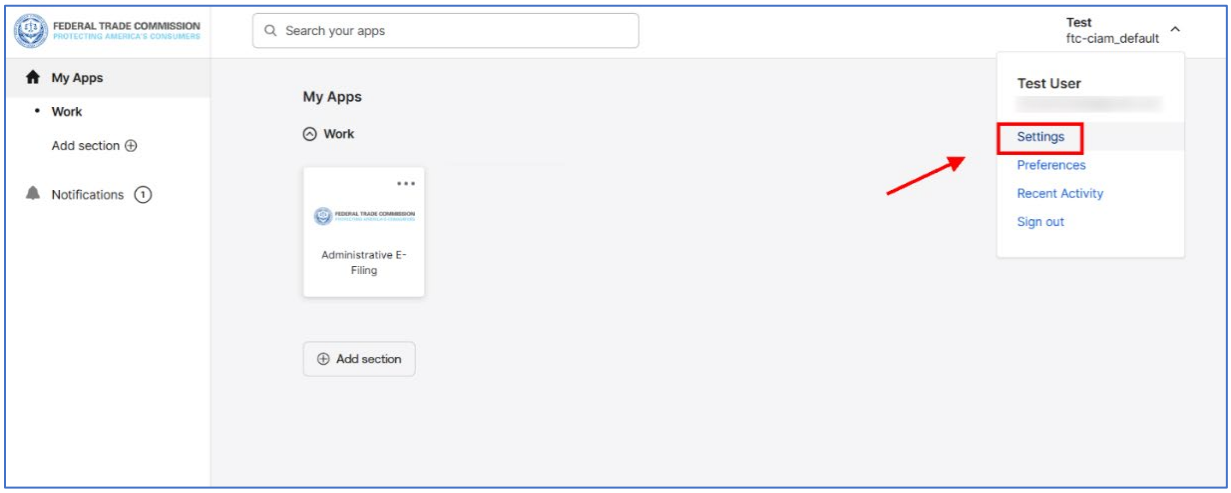
You have now successfully configured the FIDO2 (WebAuthn) Authenticator!

Your account registration with the FTC is now complete. You can now conveniently access all external FTC applications to which you have access through this account.

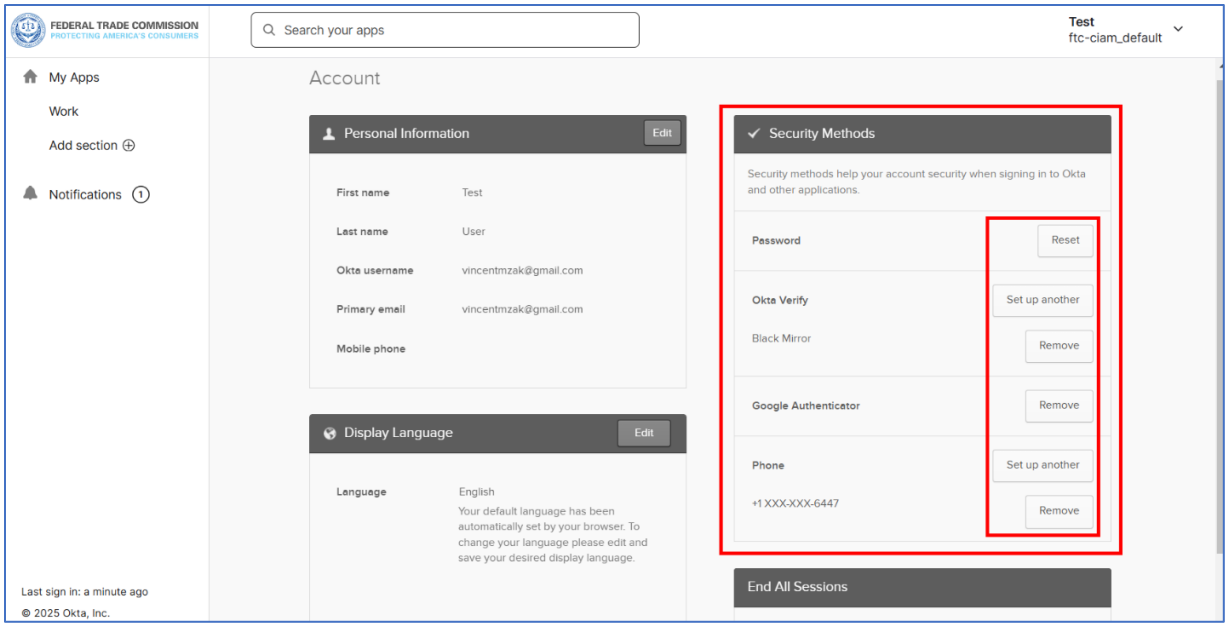
3.1.4 Updating Multi-Factor Authentication Settings

If you need to update/change your selections for Multi-factor Authentication, please follow the steps below:

1) Navigate to: https://login.ftc.gov/
2) Enter in your username and password.
3) You will be asked once again to complete the authentication process.
4) Upon successful authentication, you will see the below screen:



5) Click on your Account and then “Settings”.
6) Here you will have the option to make changes to your account, please click on the option you would like to change and proceed.

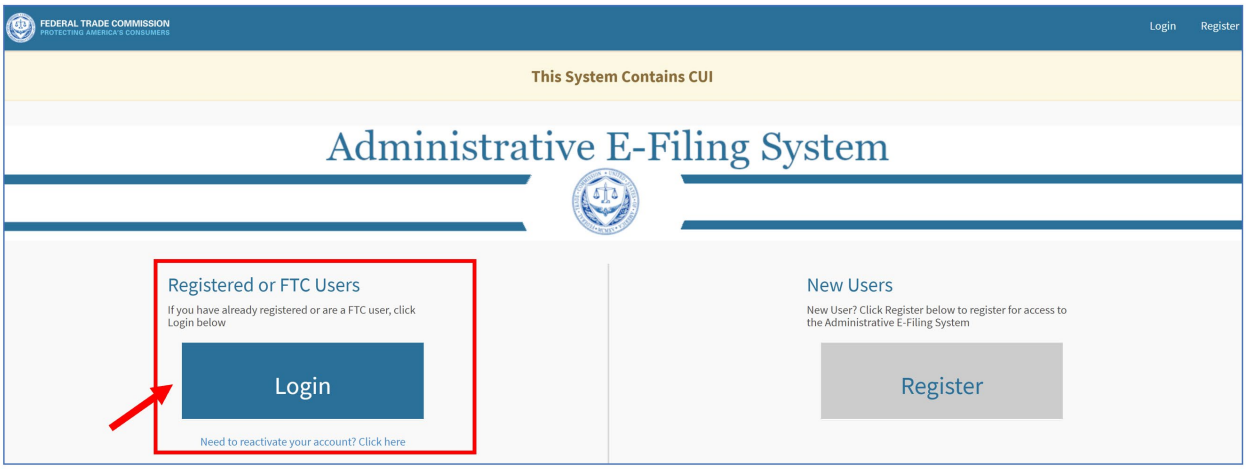


3.2 Registered Users

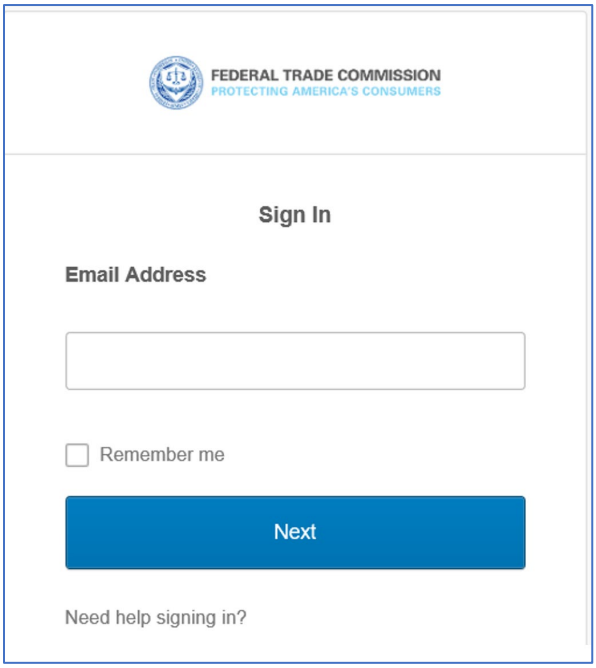
3.2.1 Login

If you have previously registered with the FTC, you can access the Administrative E-Filing System by going to **https://adminefiling.ftc.gov**.

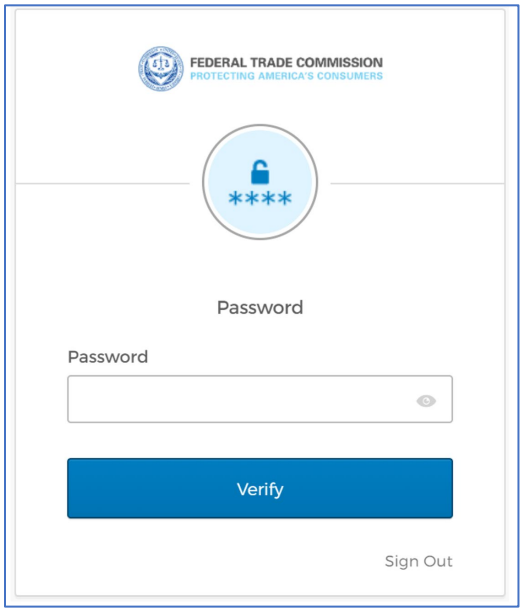
Click "Login" under Registered Users and enter the e-mail address and password associated with the registered user account.



Enter your email address and click “Next”.

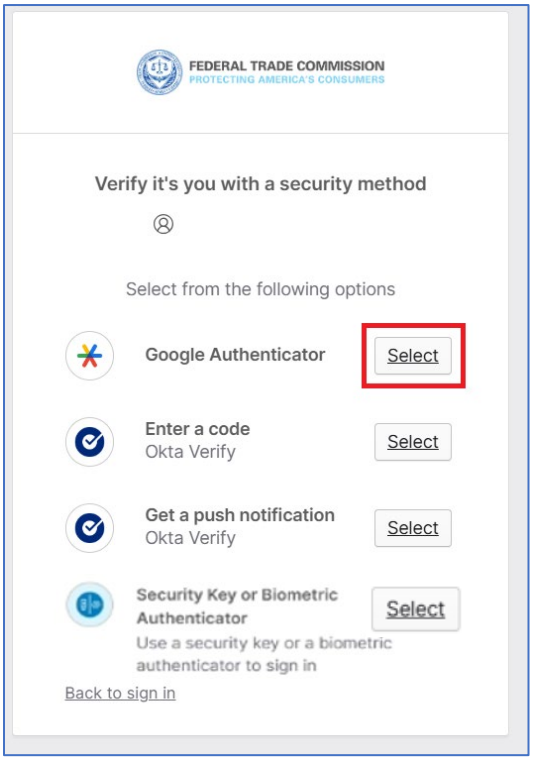


Then, enter in your password and click “Verify”.

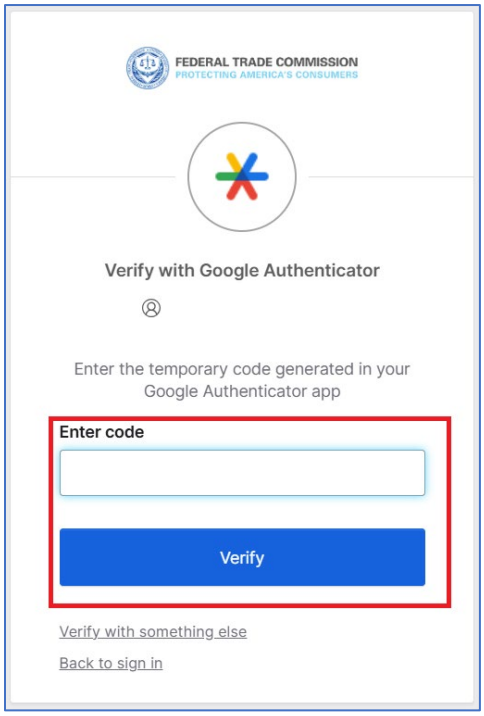


You will then be prompted to complete the authentication process. Please proceed with either “Okta Verify”, “Google Authenticator”, or “Security Key or Biometric Authentication”.

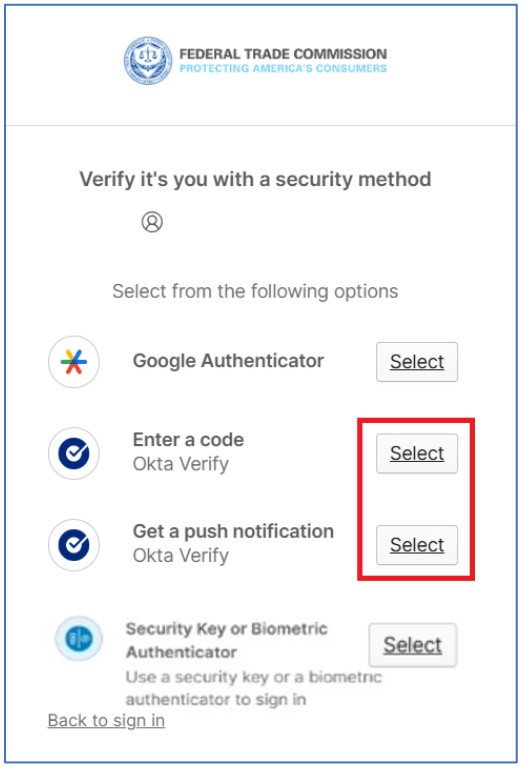
If you want to use “Google Authenticator”, push “Select”.



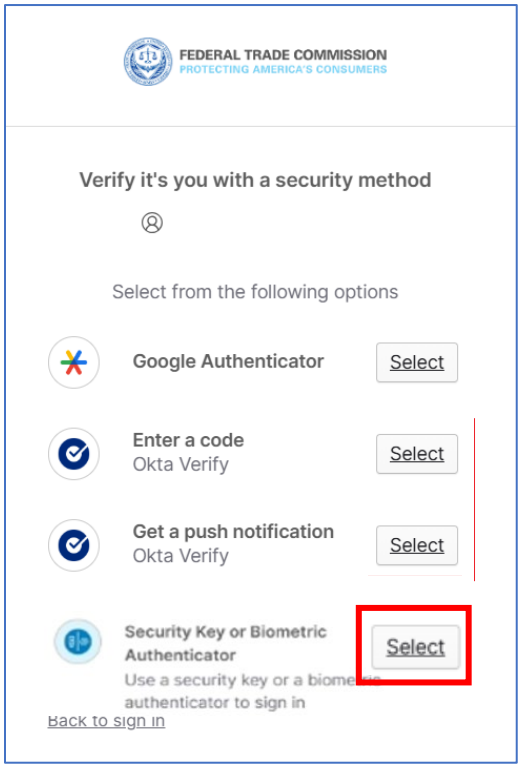
Now open Google Authenticator and enter the rolling One Time Password (OTP) and select “Verify”.



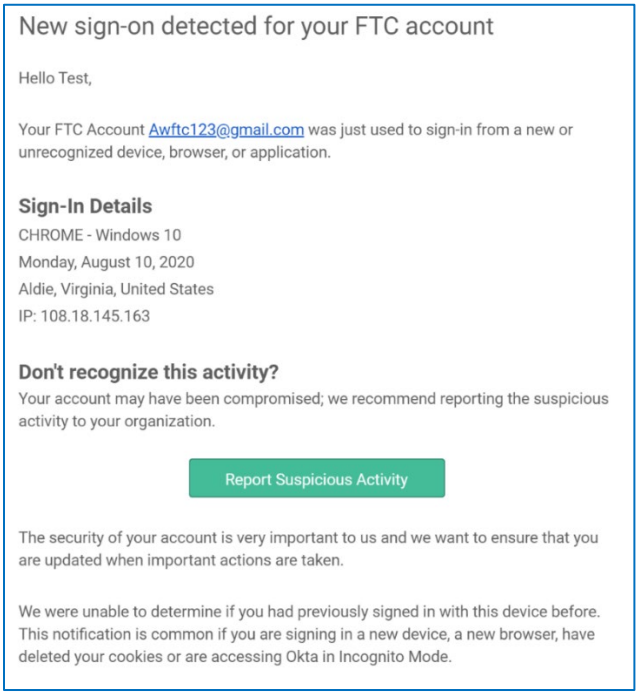
If want to use “Okta Verify”, select “Enter a Code” or “Get a Push Notification”—**Push Notification is the suggested method**. Open your mobile device and push the prompt.



If want to use “Security Key or Biometric Authentication,” click “Select”.



Upon successful authentication, you will be logged in to the application and you will receive an email notification confirming your login.



New sign-on detected for your FTC account

Hello Test,

Your FTC Account Awftc123@gmail.com was just used to sign-in from a new or unrecognized device, browser, or application.

Sign-In Details

CHROME - Windows 10
Monday, August 10, 2020
Aldie, Virginia, United States
IP: 108.18.145.163

Don't recognize this activity?

Your account may have been compromised; we recommend reporting the suspicious activity to your organization.

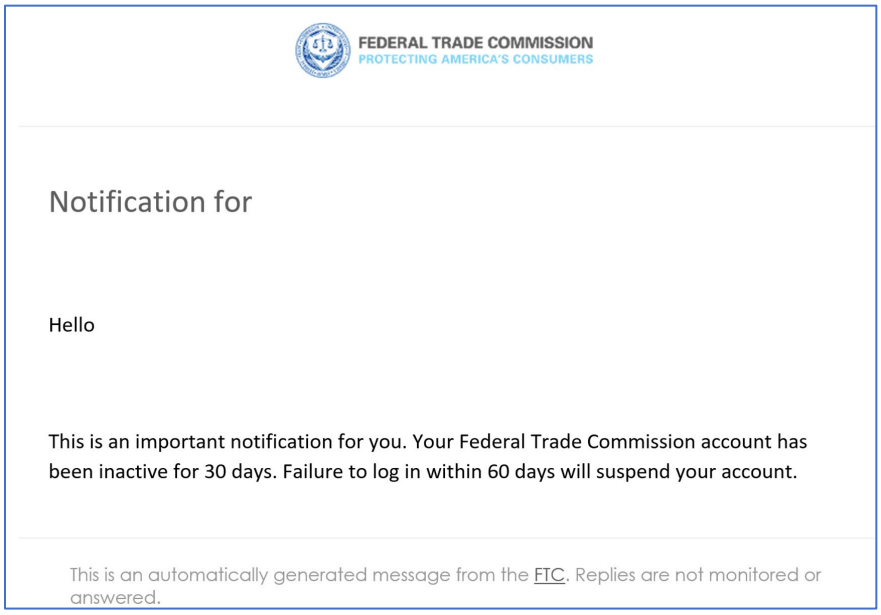
Report Suspicious Activity

The security of your account is very important to us and we want to ensure that you are updated when important actions are taken.

We were unable to determine if you had previously signed in with this device before. This notification is common if you are signing in a new device, a new browser, have deleted your cookies or are accessing Okta in Incognito Mode.

3.2.2 Reactivate Account

Your account will be automatically deactivated after 90 days of inactivity. You will receive emails at 30, 60 and 83 days of inactivity reminding that you need to login to keep your account active. Sample reminder email at 30 days is shown below:



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

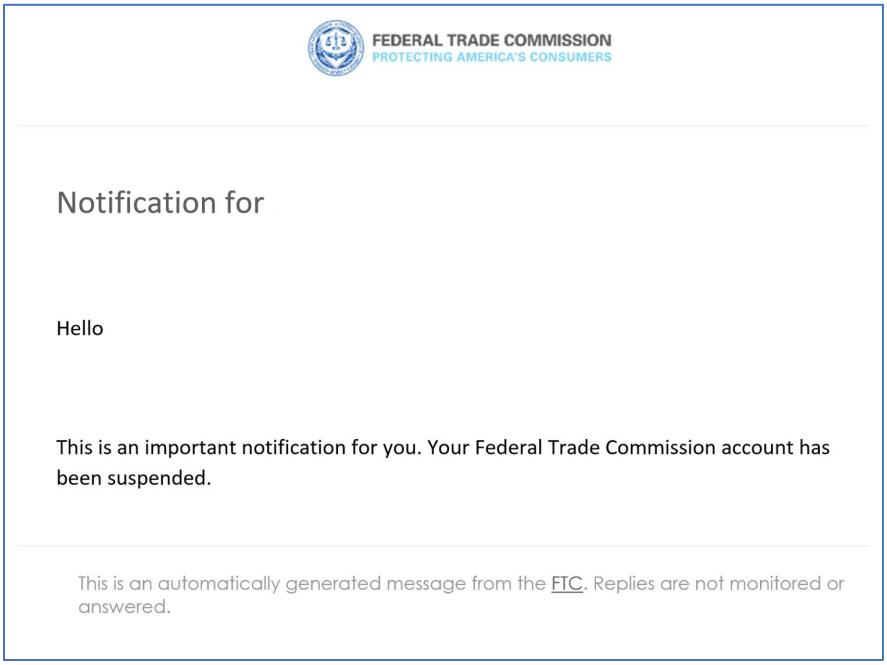
Notification for

Hello

This is an important notification for you. Your Federal Trade Commission account has been inactive for 30 days. Failure to log in within 60 days will suspend your account.

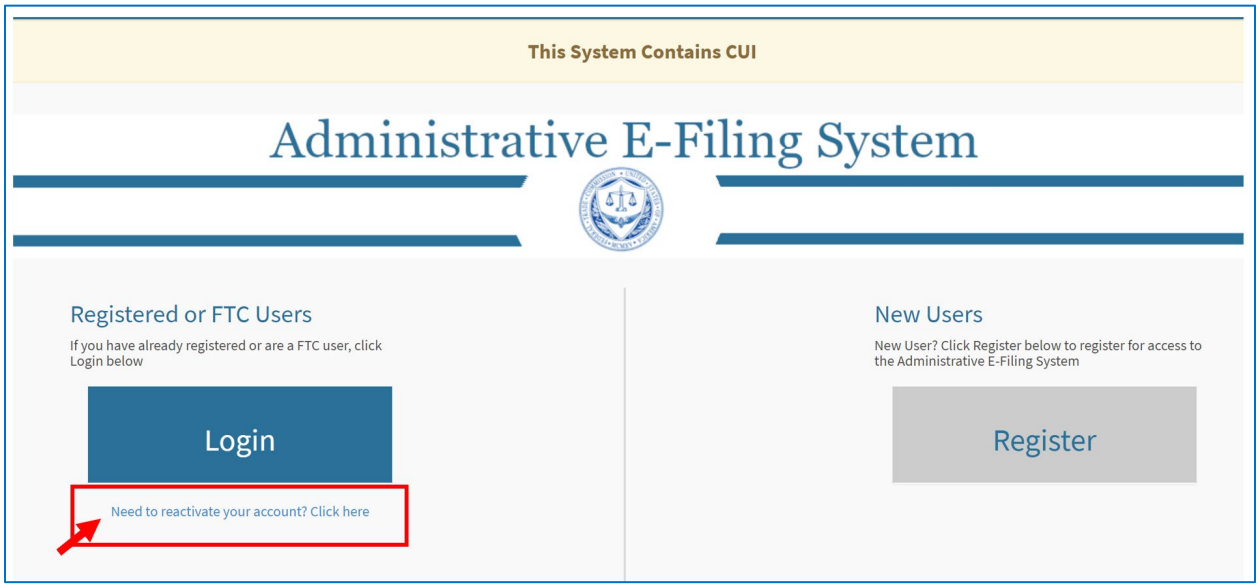
This is an automatically generated message from the FTC. Replies are not monitored or answered.

If you do not have activity in your account at 90 days, it will be automatically deactivated and you will receive the following email notification:



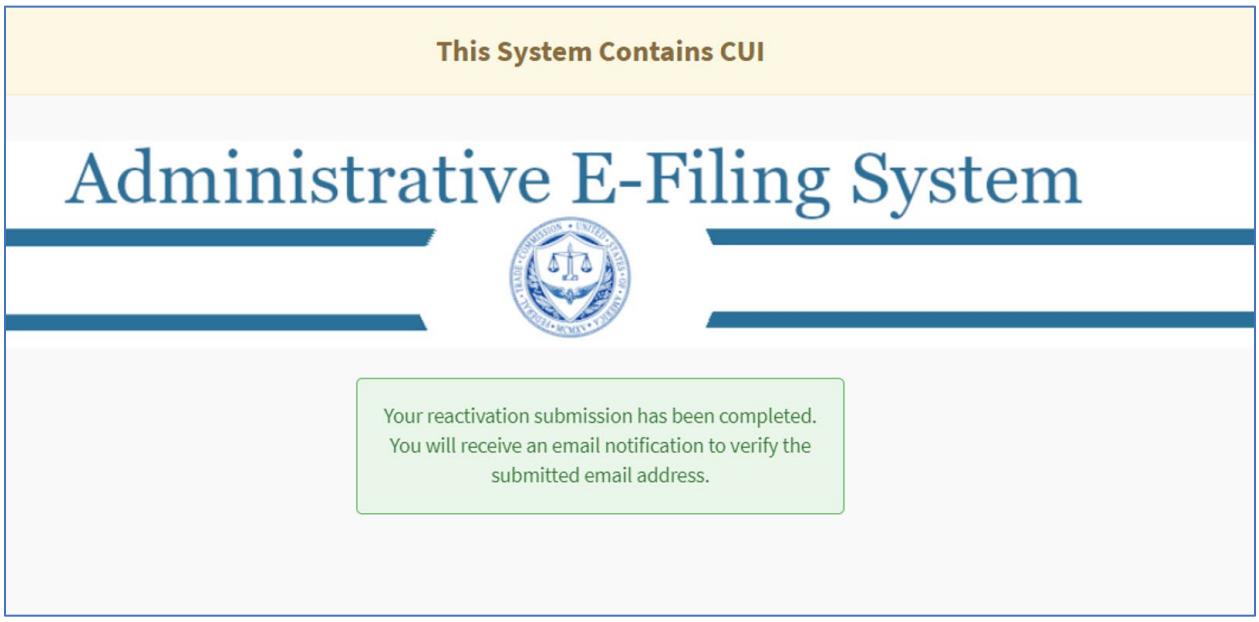
If your account has been deactivated and you need to reactivate it, please click on "Reactivate account" as shown below.

Navigate to https://adminefiling.ftc.gov/ftcefile and click on the link to reactivate your account that is below the "Login" button:

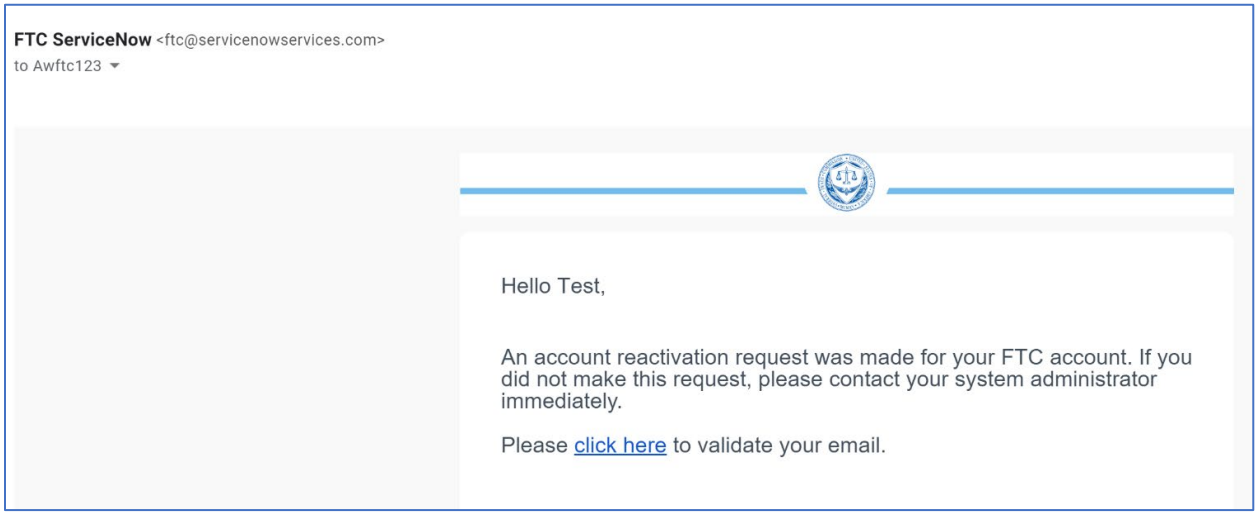


You will be taken to the reactivation page. Enter your email address and click “Reactivate My Account”.

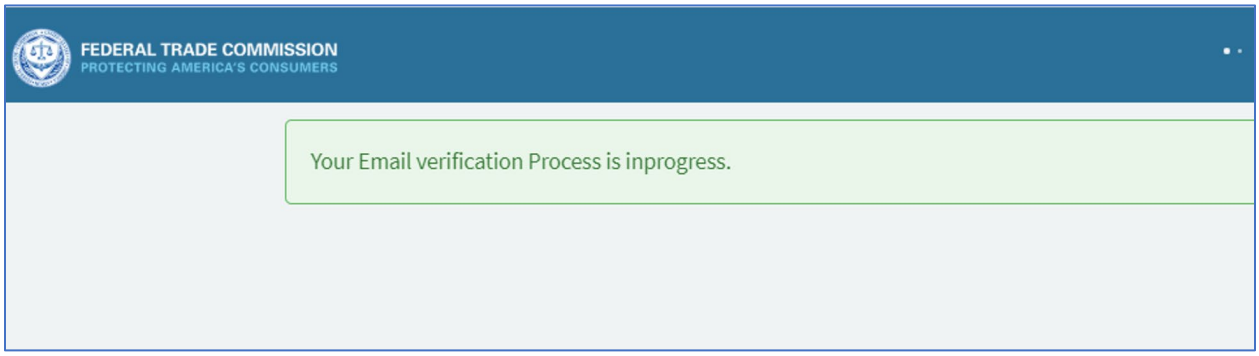
Upon entering your email address and clicking “Reactivate My Account”, you will receive the below on-screen confirmation, and you will also receive an email notification with a link to verify your account.



You will receive an email to verify your account for reactivation, please follow the instructions in the email to proceed.

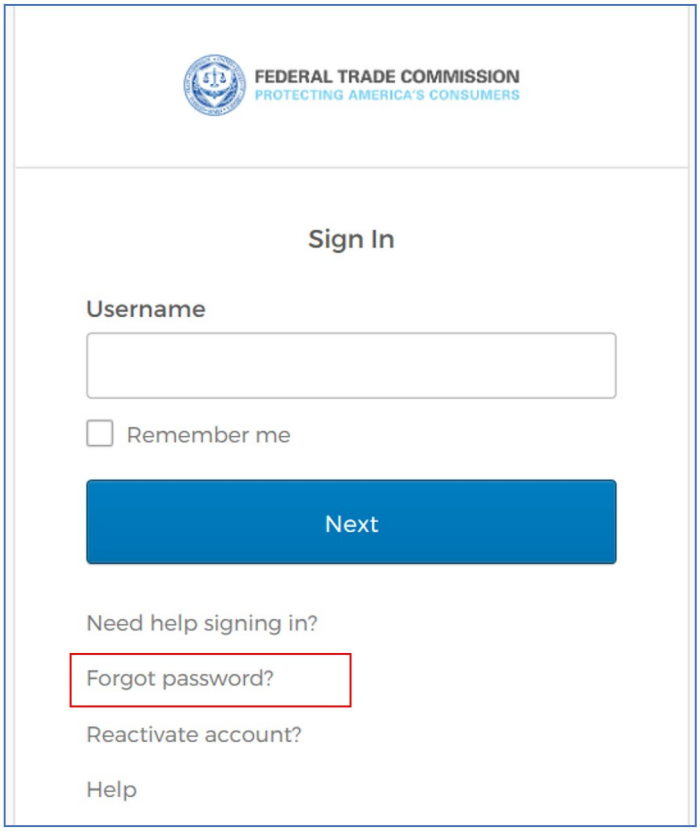


The following on-screen notification will be displayed confirming that your email verification is in progress. You will then receive another email confirming that your account has been successfully verified or if there was a problem with the verification.

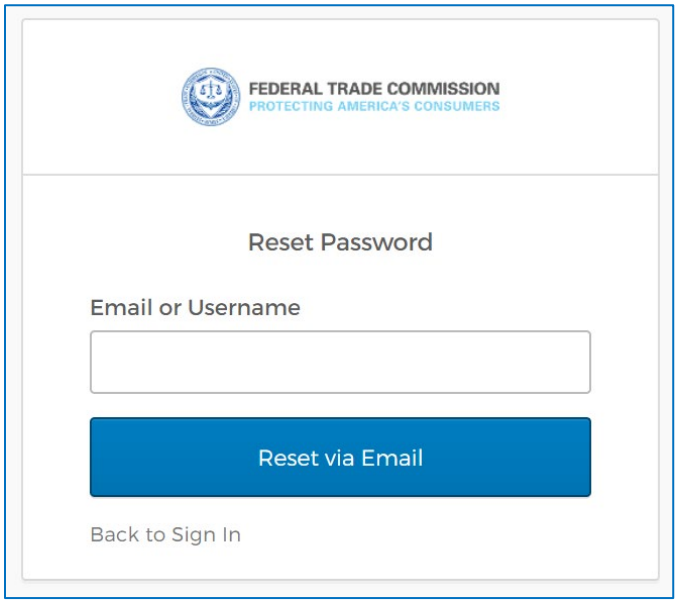


3.2.3 Reset Password

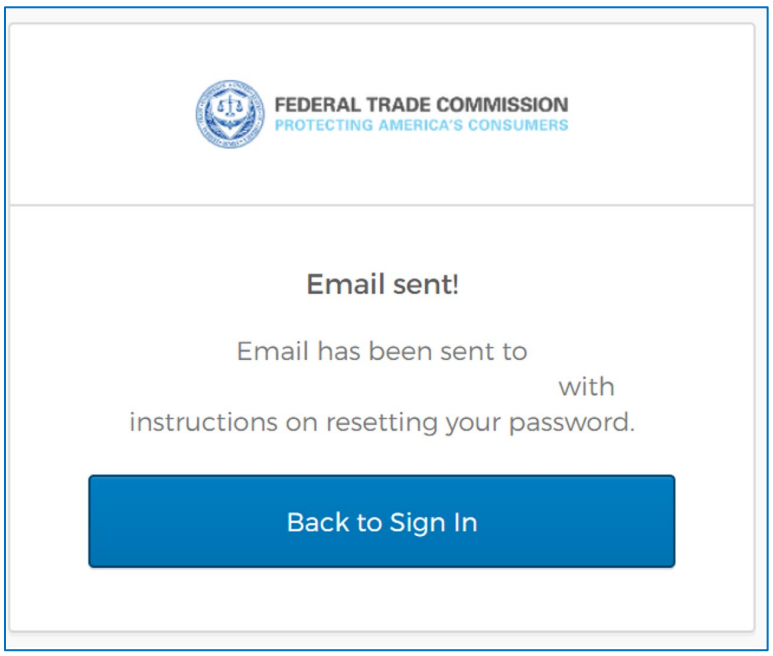
If your password needs to be reset, please click on “Forgot password” as shown below:



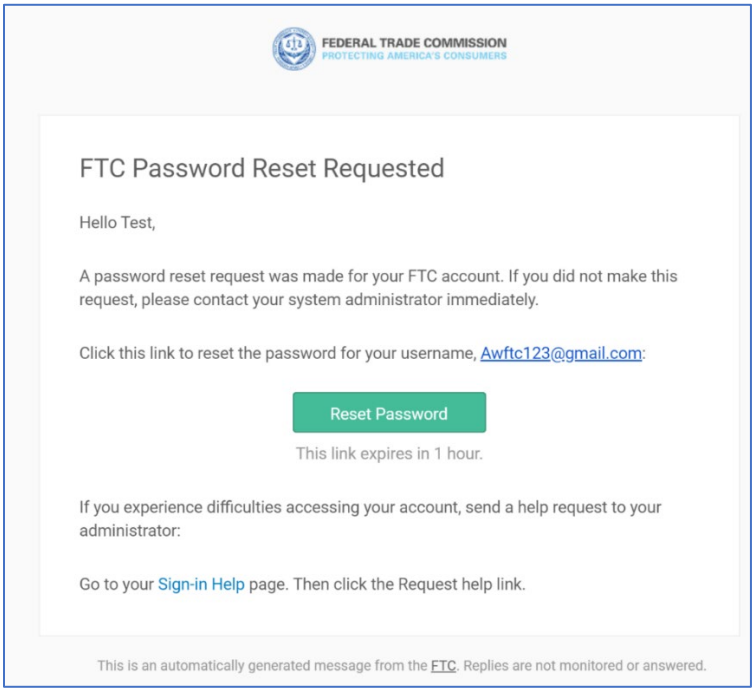
Please enter your email and click “Reset via Email”.



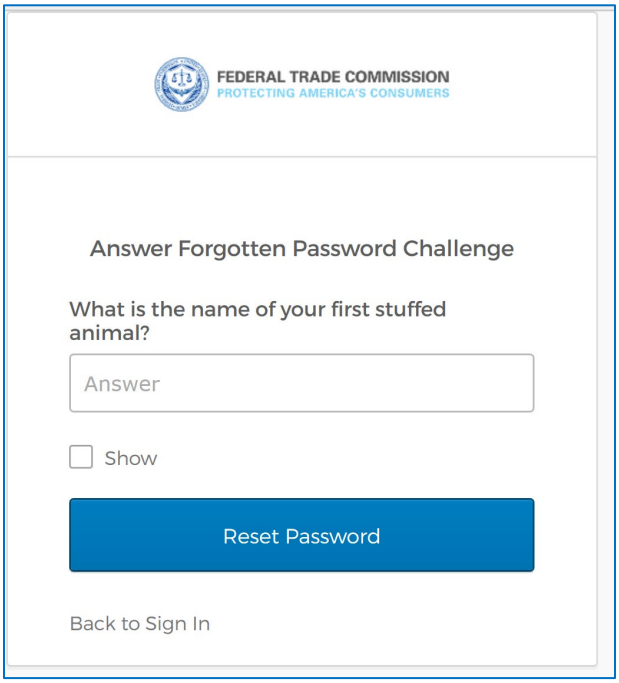
An on-screen confirmation will be displayed confirming that an email has been sent to your registered email account. Please open the email to proceed.



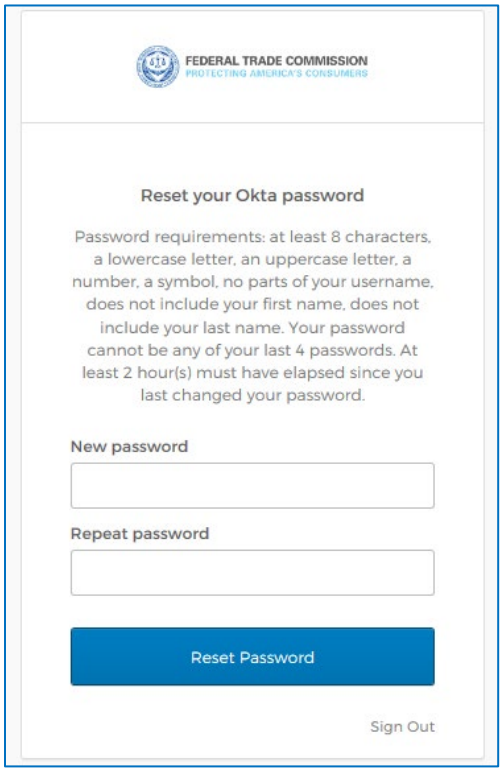
You will receive an email with a link to proceed with password reset. Please click on the "Reset Password" link.



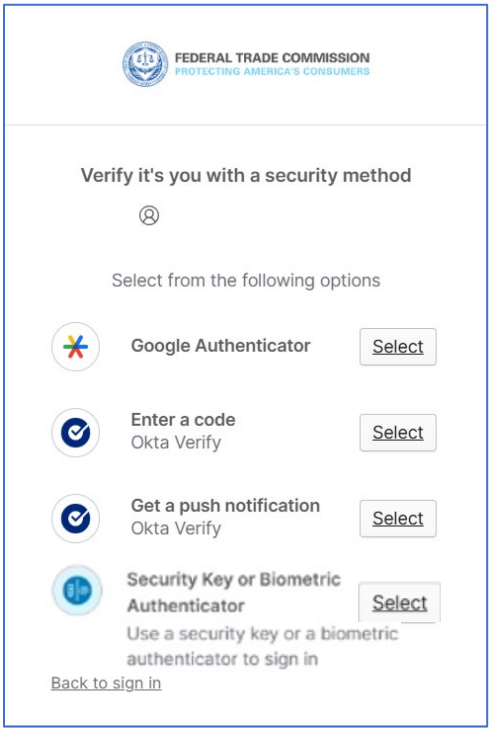
Upon clicking the link, you will be prompted to answer your security questions. Please enter in the answer and click “Reset Password”.



Please create a new password, repeat the password and click “Reset Password”.



You will be prompted to complete the multi-factor authentication process. Please select your preferred MFA factor and click “Select”.



4. Login to Administrative E-Filing

That should complete the password reset process and you should be able to login to the Admin E-Filing application: **https://adminefiling.ftc.gov**.

After logging-in, go to the Contact Us page to find the Administrative E-Filing System External User Guide for instructions on how to use the application.

5. Troubleshooting

If you need further assistance and are experiencing technical difficulty, please contact the Federal Trade Commission Technical Support Team (support.adminefiling@ftc.gov).