

FTC Registered Identification Number (RN) System External User Registration Guide

February 2026



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	7
3.1.3 Setup Multi-Factor Authentication	10
3.1.4 Updating Multi-Factor Authentication Settings.....	29
3.2 Registered Users.....	30
3.2.1 Login.....	30
3.2.2 Reactivate Account	34
4. Login to RN System.....	41
5. Troubleshooting	41

1. Introduction

The Federal Trade Commission's (FTC's) RN System is a web-based, user-friendly application that allows customers to request a Registered Identification Number (RN) for a business residing in the U.S. and engaged in the manufacture, importing, distribution, or sale of textile, wool, or fur products. The FTC's upgraded RN System Application has been created to secure, streamline, and improve efficiencies for FTC's RN System application users.

2. Overview

This RN System User Guide is an instruction manual that provides guidance on how to navigate and securely access the RN System for an optimal user experience.

3. Application/User Registration

3.1 New/First time Users

3.1.1 Registration

To access the RN System, you must first register and create an account.

Note: Only U.S.-based businesses are eligible for an RN and only users in the United States or Canada can access the system to apply for an RN.

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

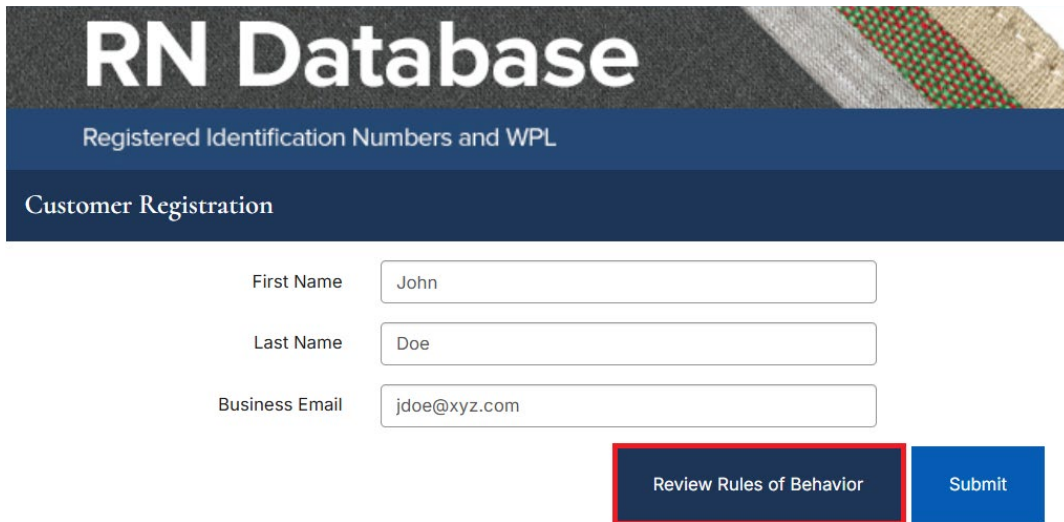
- 1) Click on the link below and then click on "Create my Account" under *Welcome*:
<https://rn.ftc.gov>

The screenshot displays the FTC RN Database website. At the top left is the FTC logo with the text "FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS". A blue banner below the logo reads "This System Contains CUI". A navigation bar contains links: "ABOUT THE FTC", "NEWS & EVENTS", "ENFORCEMENT", "POLICY", and "I WOULD LIKE TO...". The main content area features a "RN Database" header with the subtitle "Registered Identification Numbers and WPL". On the left, there are links for "RN Database", "SEARCH RN DATABASE", and "FAQ". The central text reads "Welcome to the new RN System!" followed by a message about the system upgrade. A "Create my account" button is prominent, with a link for "Or Login" below it. Further down, there are sections for "Who can apply?" and "Questions?".

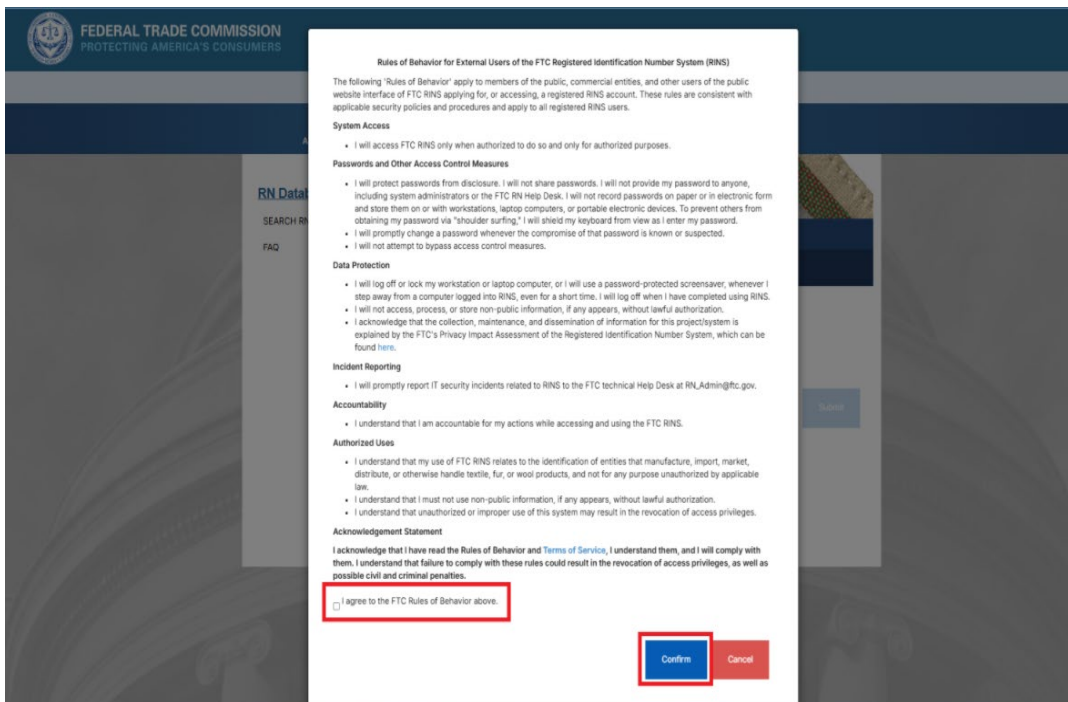
2) You will be redirected to the Customer Registration Page. To successfully complete registration, you must:

- First, enter in the requested information for each of the input fields on the Customer Registration page
- Then, click on the “**Review Rules of Behavior**” button and review the Rules thoroughly.
- After you have reviewed the rules, you must check “I agree to the FTC Rules of Behavior above” and select “Confirm”.
- Finally, click on “Submit” to complete the registration process

PLEASE NOTE: All users MUST click to acknowledge the Rules of Behavior to continue the registration process.



The image shows a registration form for the RN Database. The header includes the text "RN Database" and "Registered Identification Numbers and WPL". Below this is a section for "Customer Registration" with three input fields: "First Name" (containing "John"), "Last Name" (containing "Doe"), and "Business Email" (containing "jdoe@xyz.com"). At the bottom right of the form are two buttons: "Review Rules of Behavior" (highlighted with a red border) and "Submit" (highlighted in blue).



This image displays the "Rules of Behavior for External Users of the FTC Registered Identification Number System (RINS)" page. The page is part of the Federal Trade Commission's website, as indicated by the logo and text "FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS". The main content area contains the following sections:

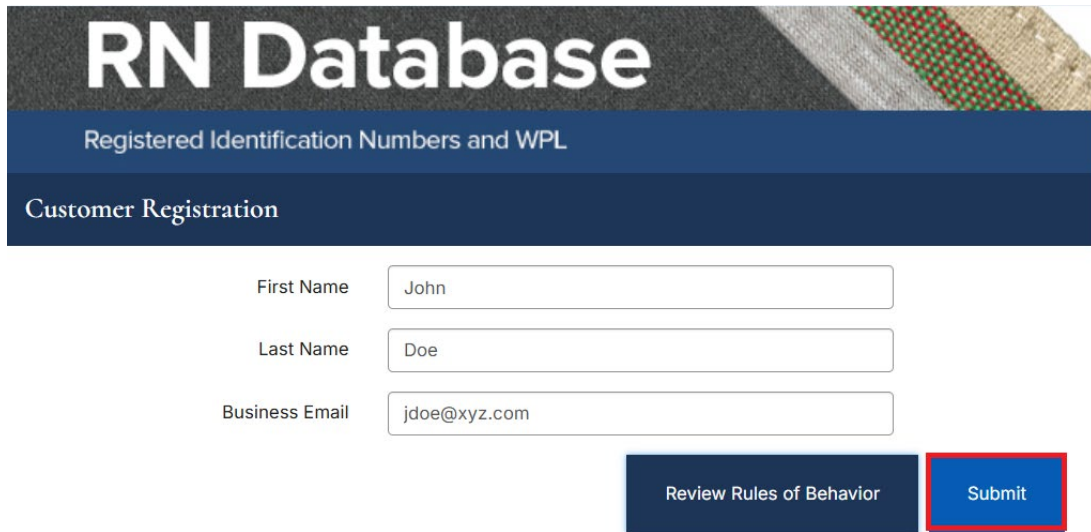
- Rules of Behavior for External Users of the FTC Registered Identification Number System (RINS)**

The following "Rules of Behavior" apply to members of the public, commercial entities, and other users of the public website interface of FTC RINS applying for, or accessing, a registered RINS account. These rules are consistent with applicable security policies and procedures and apply to all registered RINS users.
- System Access**
 - I will access FTC RINS only when authorized to do so and only for authorized purposes.
- Passwords and Other Access Control Measures**
 - I will protect passwords from disclosure. I will not share passwords. I will not provide my password to anyone, including system administrators or the FTC RN Help Desk. I will not record passwords on paper or in electronic form and store them on or with workstations, laptop computers, or portable electronic devices. To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.
 - I will promptly change a password whenever the compromise of that password is known or suspected.
 - I will not attempt to bypass access control measures.
- Data Protection**
 - I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from a computer logged into RINS, even for a short time. I will log off when I have completed using RINS.
 - I will not access, process, or store non-public information, if any appears, without lawful authorization.
 - I acknowledge that the collection, maintenance, and dissemination of information for this project/system is explained by the FTC's Privacy Impact Assessment of the Registered Identification Number System, which can be found [here](#).
- Incident Reporting**
 - I will promptly report IT security incidents related to RINS to the FTC technical Help Desk at RN_Admin@ftc.gov.
- Accountability**
 - I understand that I am accountable for my actions while accessing and using the FTC RINS.
- Authorized Uses**
 - I understand that my use of FTC RINS relates to the identification of entities that manufacture, import, market, distribute, or otherwise handle textile, fur, or wool products, and not for any purpose unauthorized by applicable law.
 - I understand that I must not use non-public information, if any appears, without lawful authorization.
 - I understand that unauthorized or improper use of this system may result in the revocation of access privileges.
- Acknowledgement Statement**

I acknowledge that I have read the Rules of Behavior and Terms of Service, I understand them, and I will comply with them. I understand that failure to comply with these rules could result in the revocation of access privileges, as well as possible civil and criminal penalties.

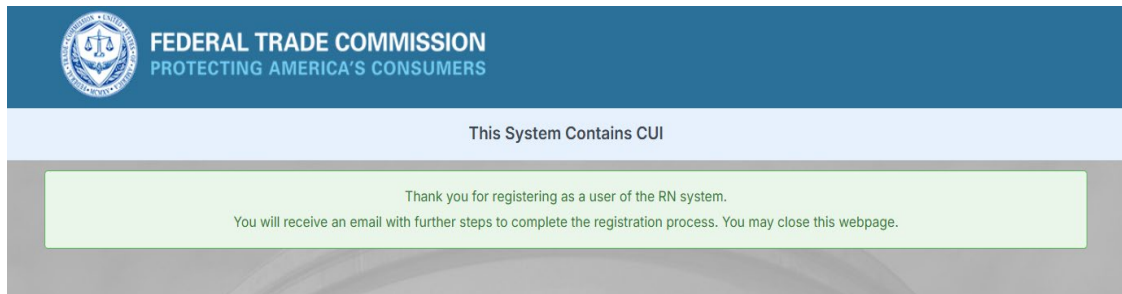
I agree to the FTC Rules of Behavior above.

At the bottom right of the page, there are two buttons: "Confirm" (highlighted with a red border) and "Cancel" (highlighted in red).



The image shows a registration form for the RN Database. The header includes the text "RN Database" and "Registered Identification Numbers and WPL". Below this is a section titled "Customer Registration". The form contains three input fields: "First Name" with the value "John", "Last Name" with the value "Doe", and "Business Email" with the value "jdoe@xyz.com". At the bottom right of the form are two buttons: "Review Rules of Behavior" and "Submit". The "Submit" button is highlighted with a red border.

- 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 Your FTC RN System Account” button to activate your account.

Welcome!

You're on the Way to Activating Your New FTC RN System Account

Hi Vincent,

The FTC is using an identity manager to handle public access to its upgraded RN System. This manager will provide access to any FTC applications you plan to use, such as the RN System, through a single home page.

As an extra layer of security, once registered, you have 24 hours to submit a request for RN before your account will be deactivated. If you fail to submit a request within the 24 hour window and your account is locked, please contact RN_admin@ftc.gov.

Click the following button to activate your FTC RN System account:

[Activate Your FTC RN System Account](#)

This link expires in 7 days.

Your username is **vzak@ftc.gov**

Your organization's sign-in page is <https://mlogin.ftc.gov/>

If you experience difficulties accessing your account, you can send a help request to the system administrator using the link: <https://ftc-ciam.okta.com/help/login>

Upon clicking on the Activate link from your email, you will be automatically redirected to the FTC “Create your FTC account” page. Please select “Set up” for your password, then enter and repeat the password in the blanks provided, and then click Next.



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Set up security methods

Ⓜ:

Security methods help protect your Test RN Systems account by ensuring only you have access.

Required now



Password

Choose a password for your account

Set up




[Back to sign in](#)



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS



Set up password



Password requirements:

- At least 14 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Does not include your first name
- Does not include your last name
- Password can't be the same as your last 4 passwords
- At least 2 hour(s) must have elapsed since you last changed your password

Enter password

Re-enter password

Next

[Return to authenticator list](#)

[Back to sign in](#)



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)

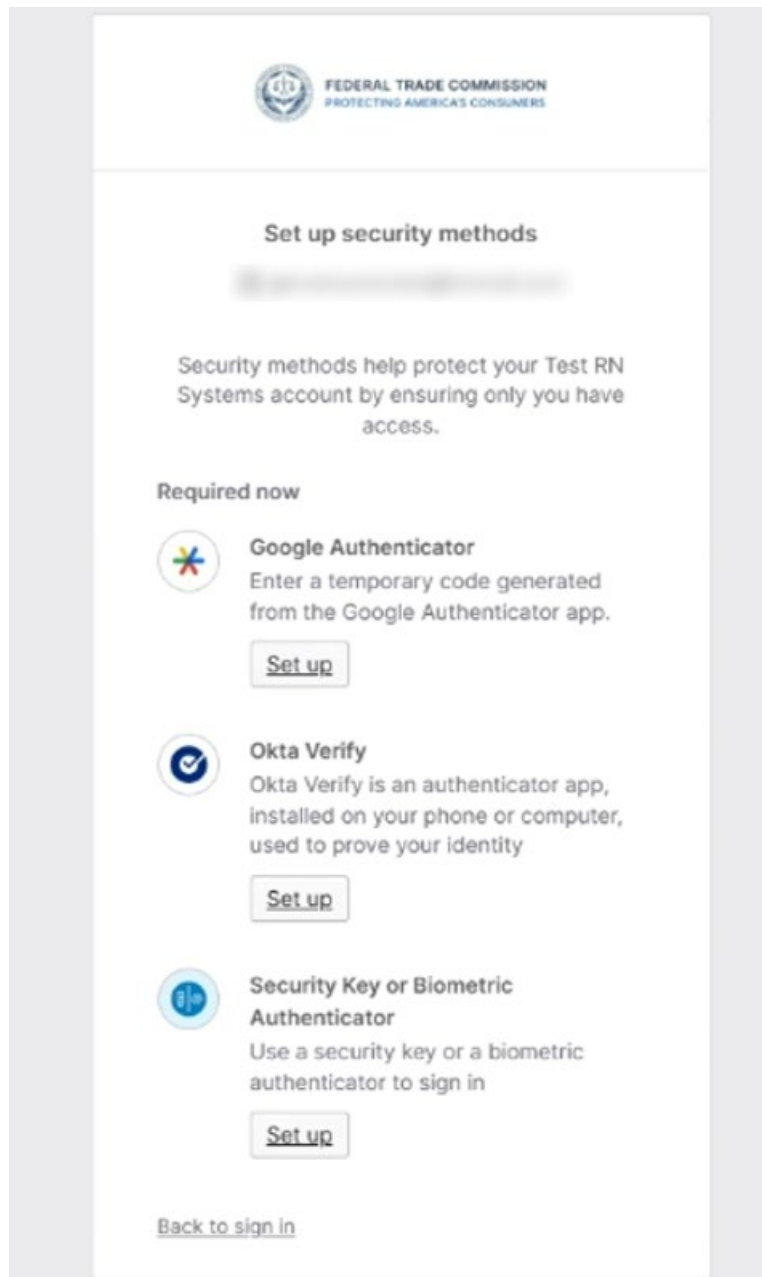
FIDO2 is the only phishing-resistant option. We suggest YubiKey 4 or higher. However, please be advised that the FTC **will not be able to provide support or resources for obtaining hardware tokens or other physical security keys or use of biometrics** for phishing-resistant MFA. While the FTC strongly 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:

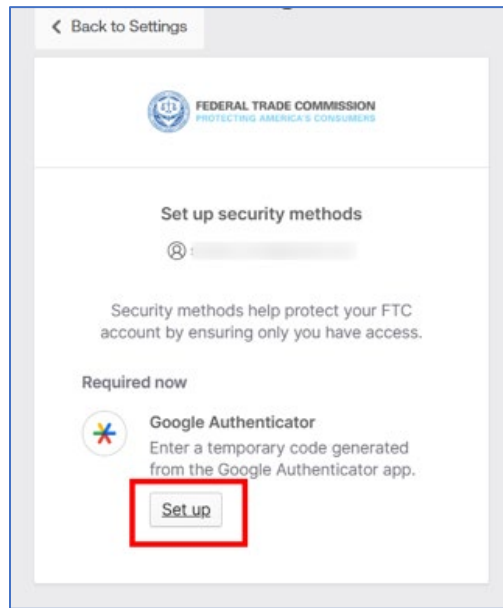
- **YubiKey** (suggested) – YubiKey 4 (2015) or higher
- **Google Titan Security Key** – USB-A and NFC; widely supported
- **Token2 T2F2 Series** – Affordable keys with USB-A, USB-C, and NFC options
- **Feitian BioPass Series** – Biometric security keys (fingerprint) with FIDO2 support
- **SoloKeys Solo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

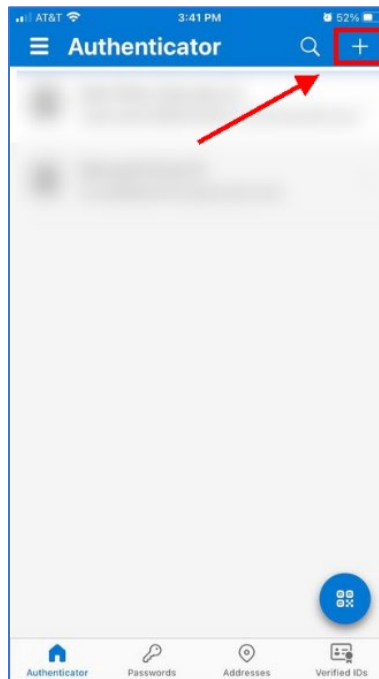


- A. If you choose “Google Authenticator”, **you will need to download the Google Authenticator App from the App Store on your mobile device to proceed via Google.**

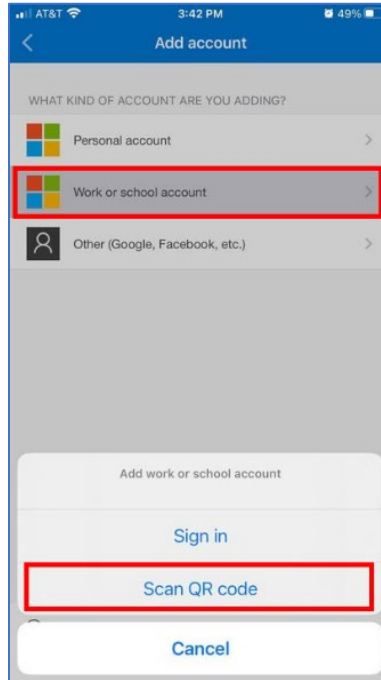


Continue by clicking “Set up”.

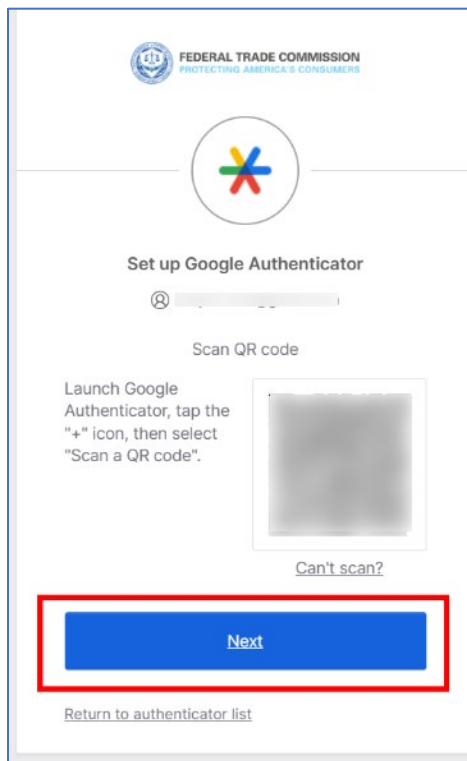
1. Open Google Authenticator app on your mobile device.
2. Select the “+”.



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”.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Set up Google Authenticator

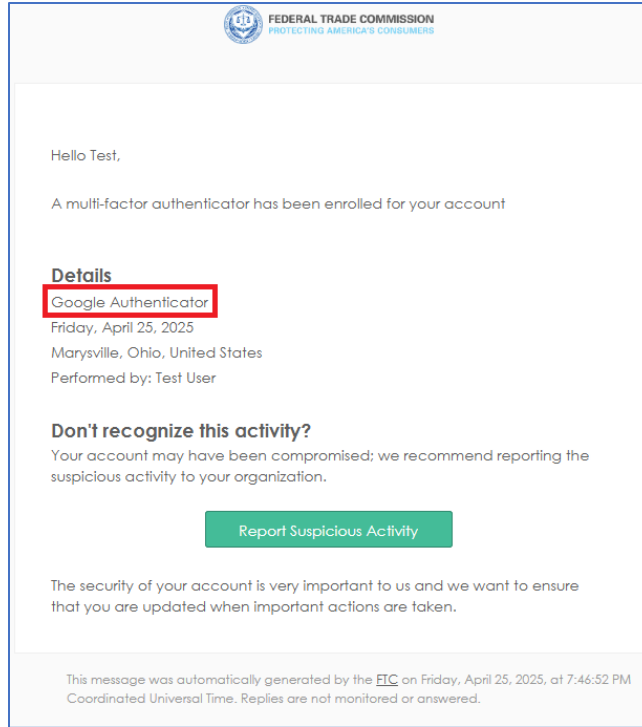
Enter code displayed from application

Enter code
112711

Verify

[Return to authenticator list](#)

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



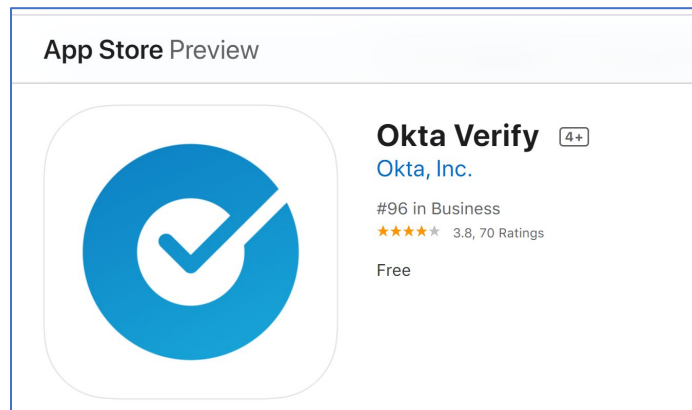
You have now successfully configured the Google Authenticator!

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.

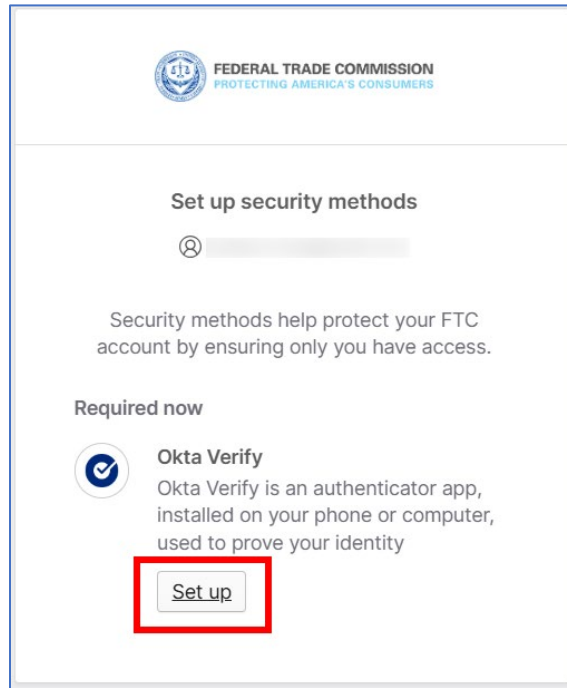
Note: As an extra layer of security, once registered, you have 24 hours to submit a request for RN before your account will be deactivated. If you fail to submit a request within the 24 hour window and your account is locked, please contact RN_admin@ftc.gov.

B. If you selected “Okta Verify”, **you will need to download the Okta Verify App from the App Store onto your mobile device to proceed via Okta.**

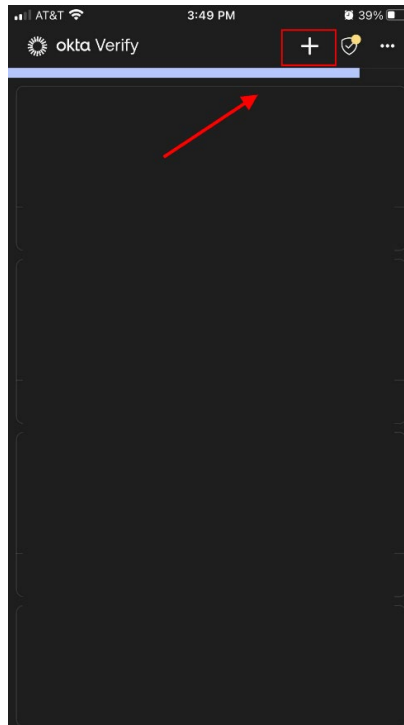
Please select your device type and click “Next”.



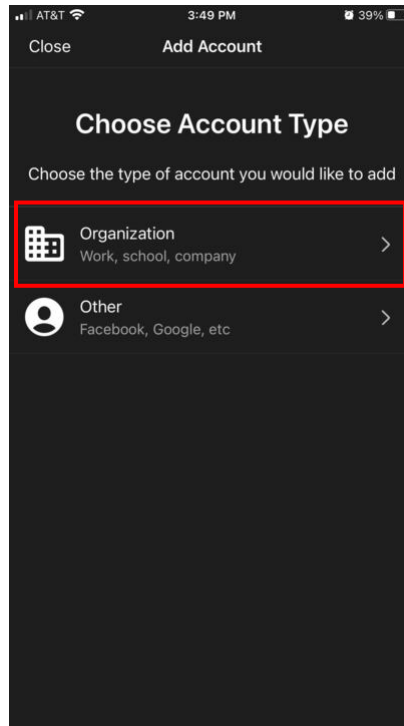
Continue by clicking “Set up” for Okta Verify.



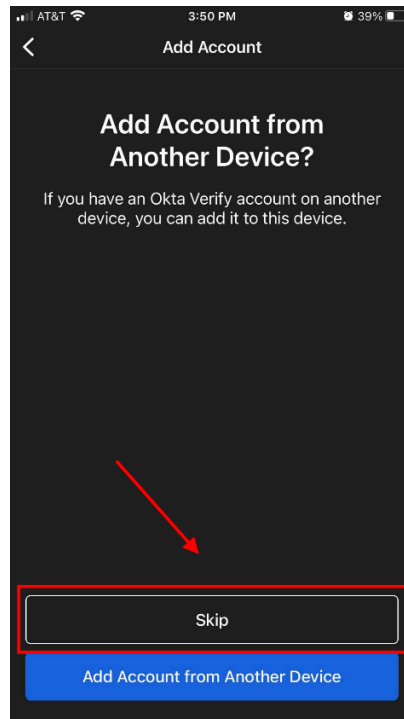
1. Open Okta Verify application on your mobile device. (Android/iPhone).
2. Select “+”.



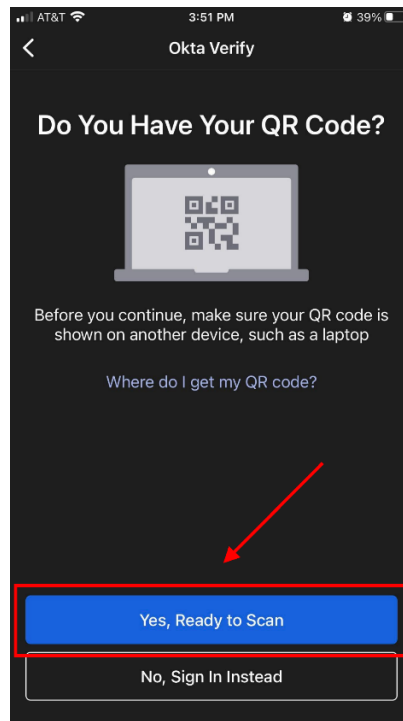
3. Select Add “Work or School Account”.



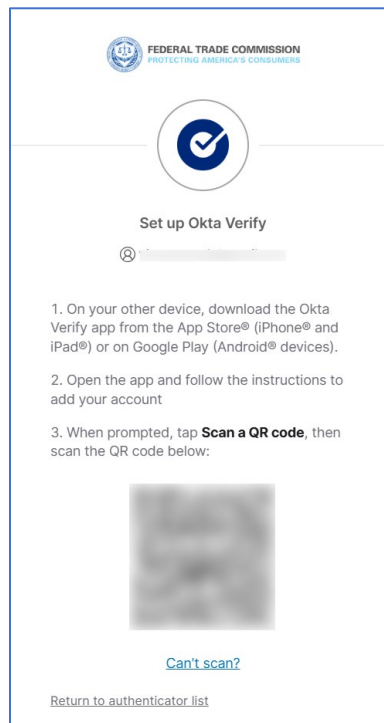
4. If you happen to have another Okta Verify account configured, you can press “Skip,” if not, then you can ignore this screen because the account you are setting up will become your default account.



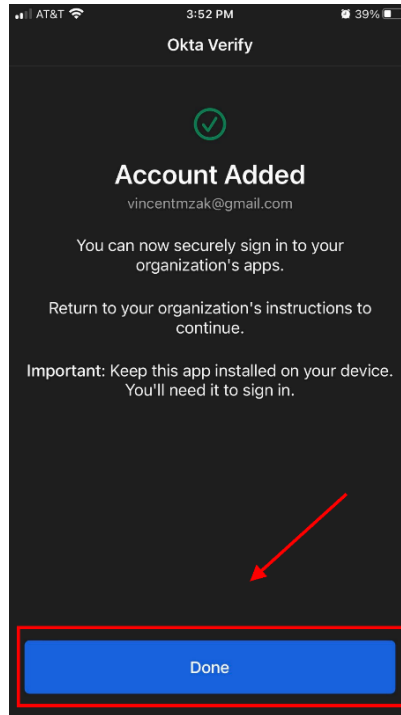
5. Select “Yes. Ready to Scan”.



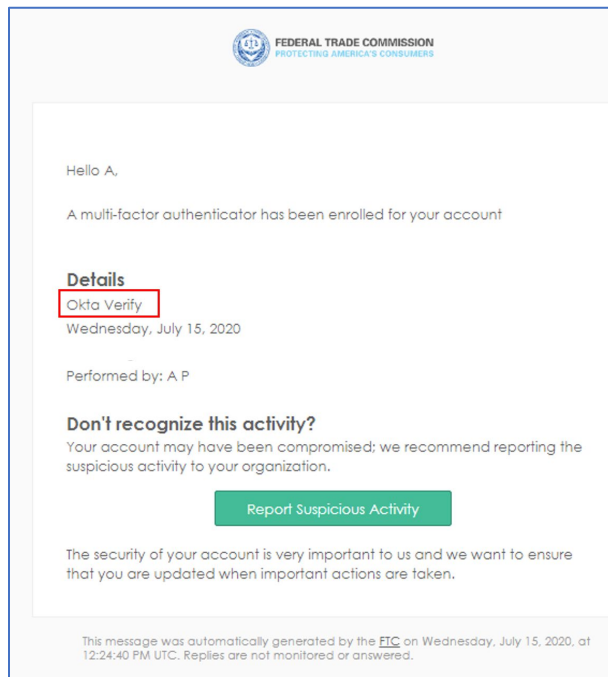
6. Okta will display a QR code on your computer screen that you will need to scan with the Okta Verify app on your mobile device.



- 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”.



- 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.

Note: As an extra layer of security, once registered, you have 24 hours to submit a request for RN before your account will be deactivated. If you fail to submit a request within the 24 hour window and your account is locked, please contact RN_admin@ftc.gov.

- 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.

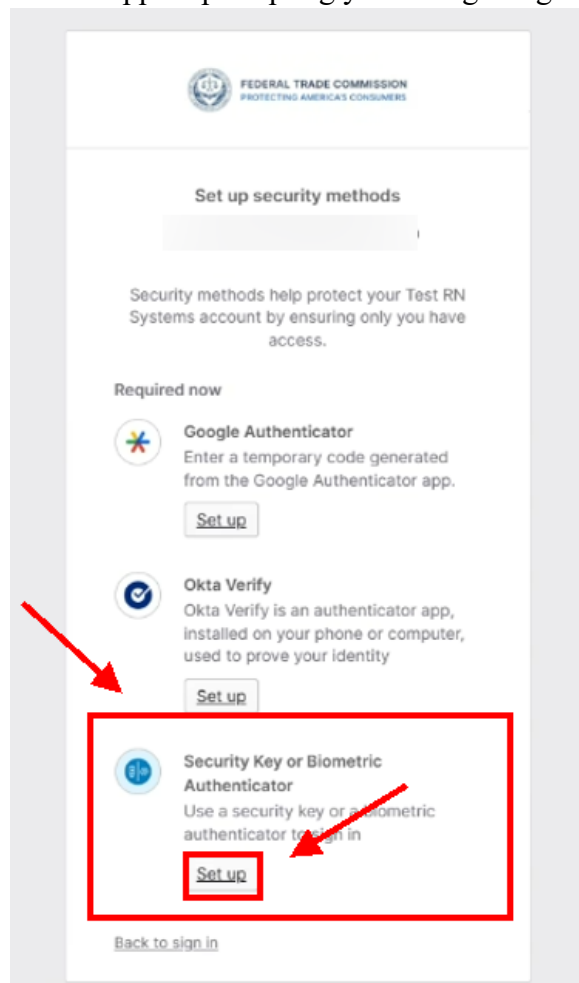
If using Biometric Authenticator enrollment, you will need to have already set it up on your computer based upon your computer’s system requirements.

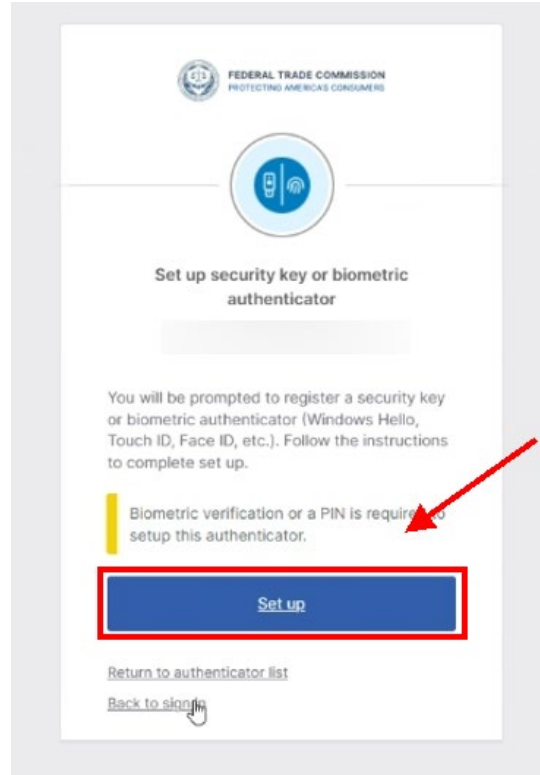
Note: If you are unable to setup or use your security key or biometrics, please select another MFA option.

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

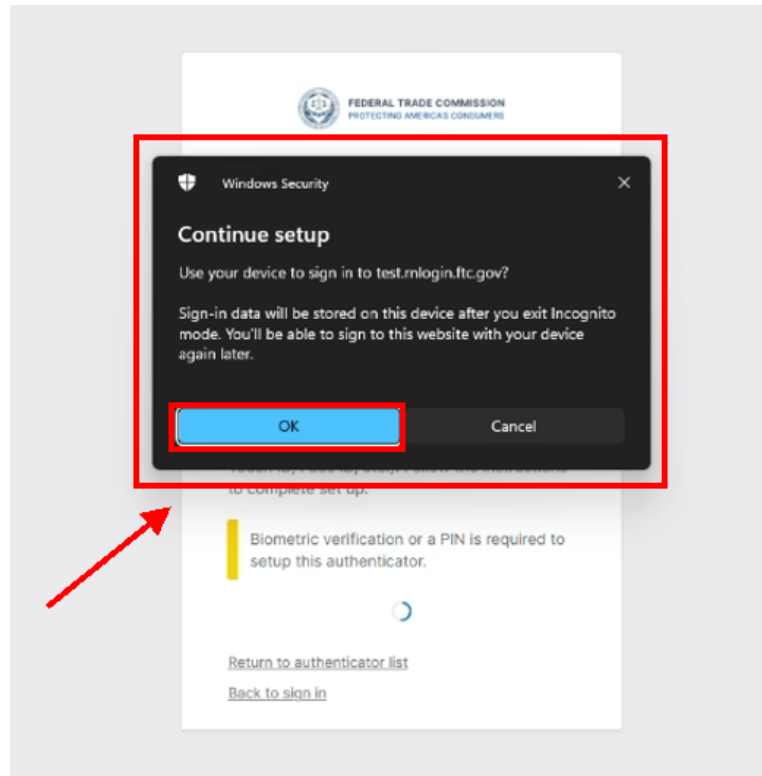
1. You must have a YubiKey 4 (2015) or higher.
2. Look for the option called “Security Key or Biometric Authenticator”, also known as FIDO2 (WebAuthn).
3. Click “Set up”.
4. A popup or new window will appear prompting you to begin registration.



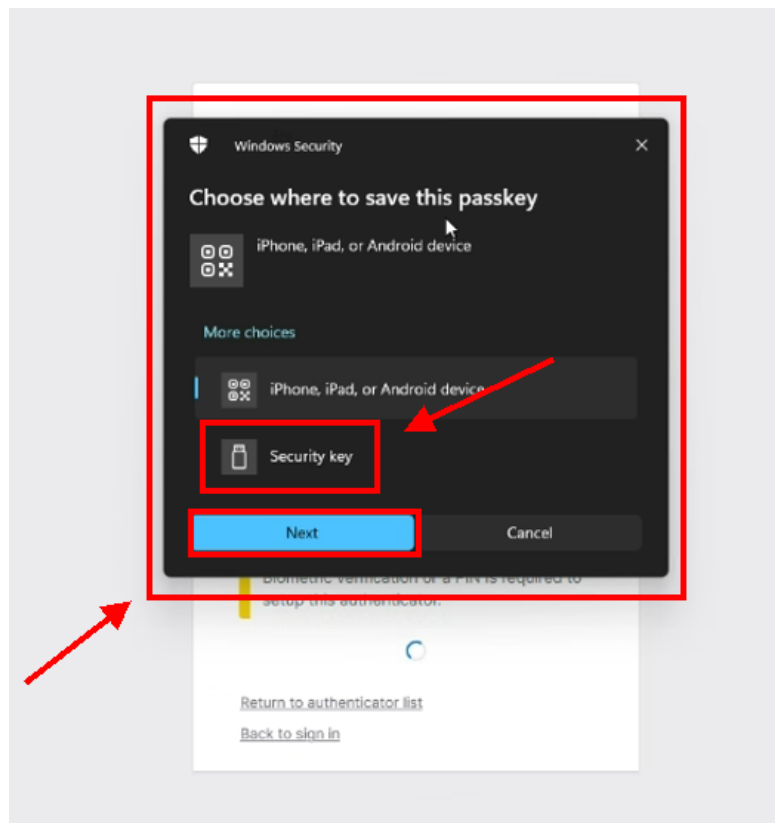


Step 2: Insert and Register Your YubiKey

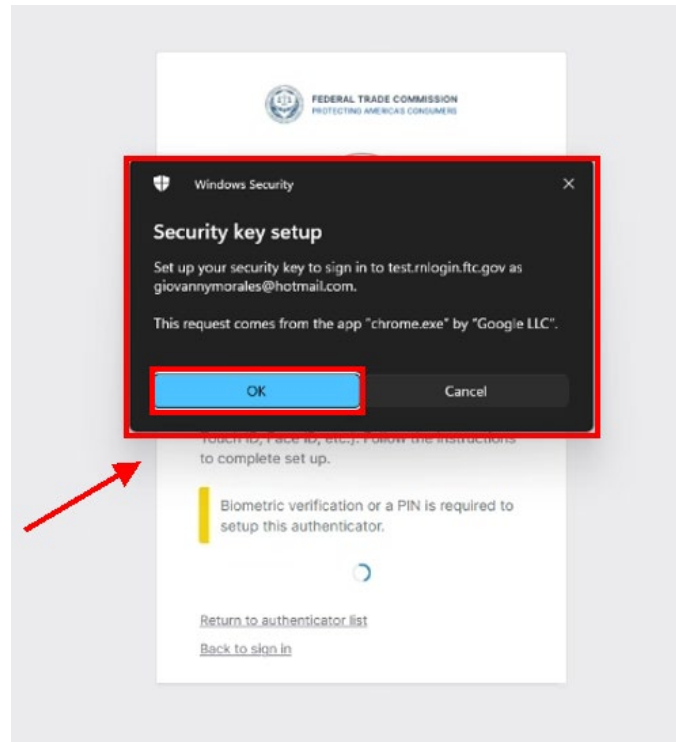
1. Insert your YubiKey into a USB port (or tap it to your device if using NFC).
2. Follow the browser prompt.
3. Touch the metal contact on your YubiKey when prompted.
4. Your browser and Okta will complete the registration.
5. You may be asked to give your key a nickname (e.g., “Work YubiKey”).
6. Select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



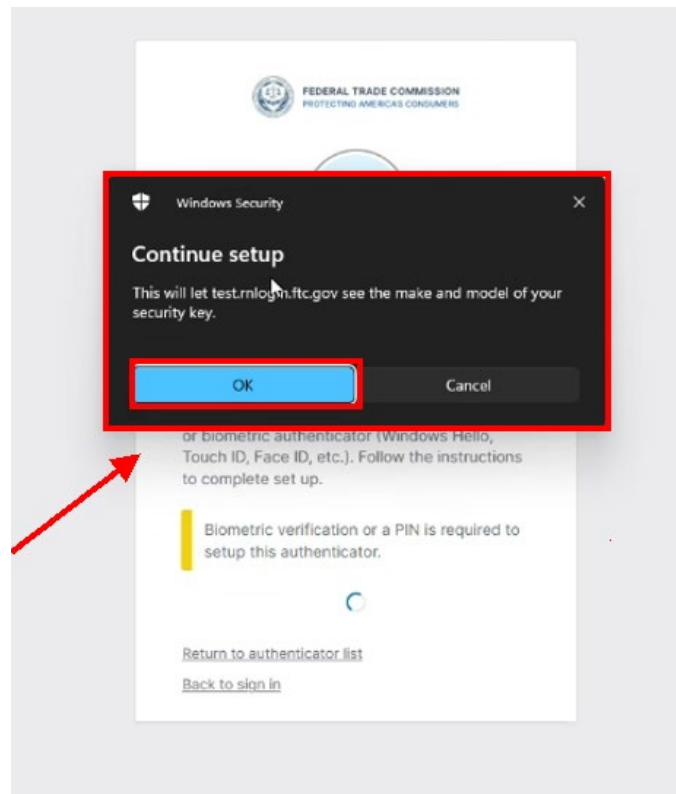
Click "OK" for the "Security Key Setup".



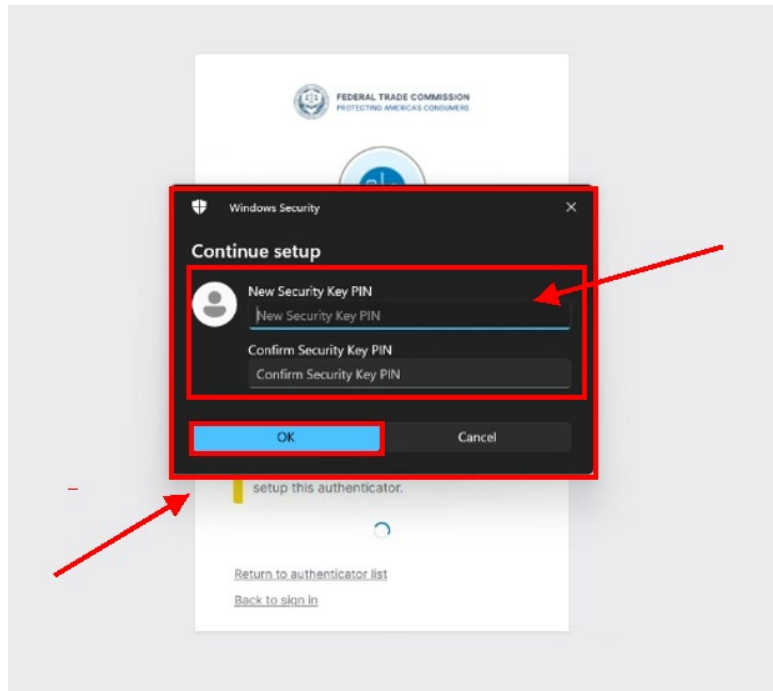
Click “OK”.



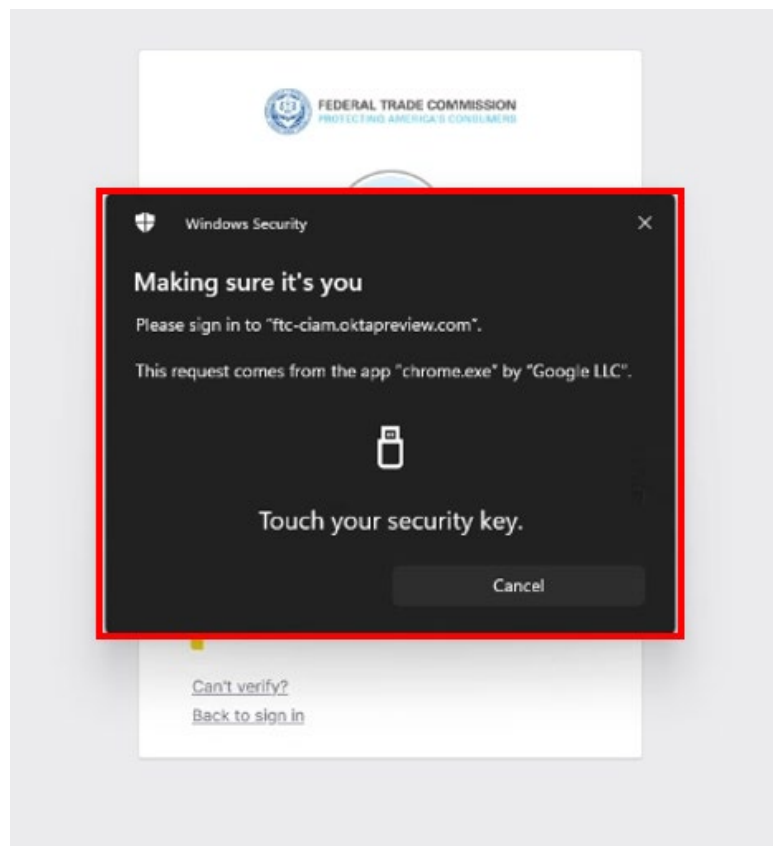
Click “OK” to Continue Setup.



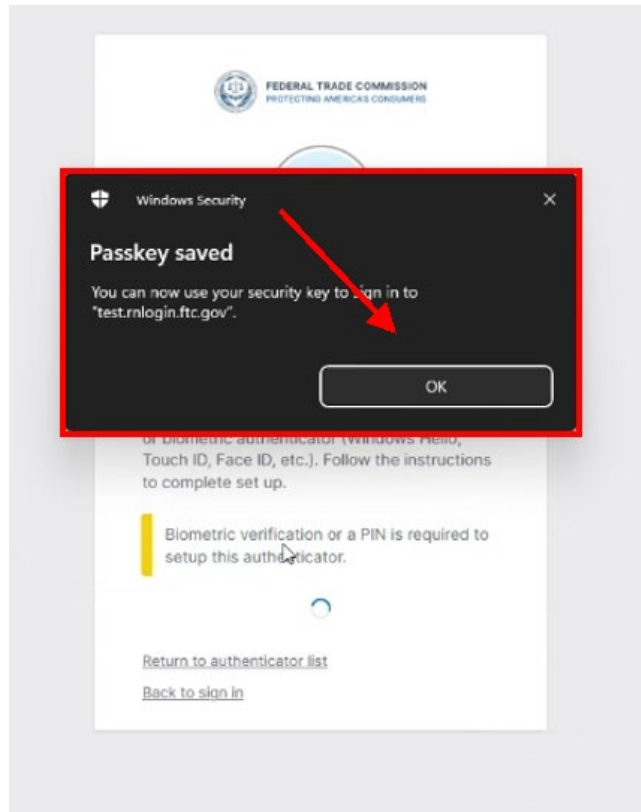
Enter a “PIN” and confirm the “PIN” number, select “OK”.



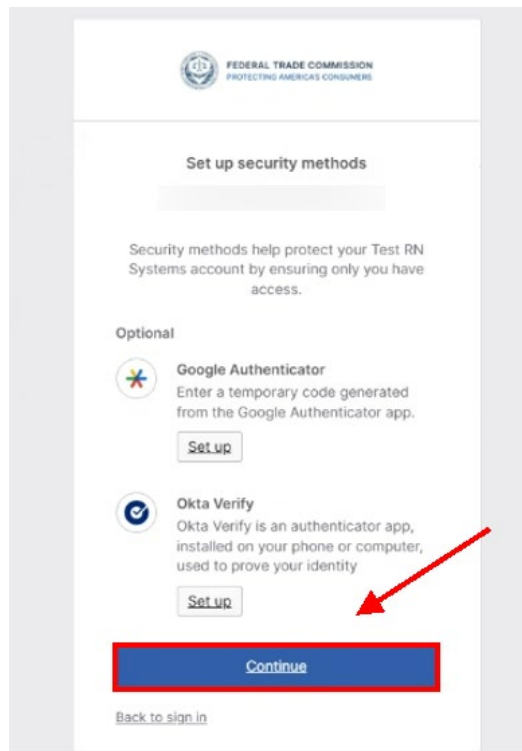
You will then be prompted to touch your “YubiKey”.

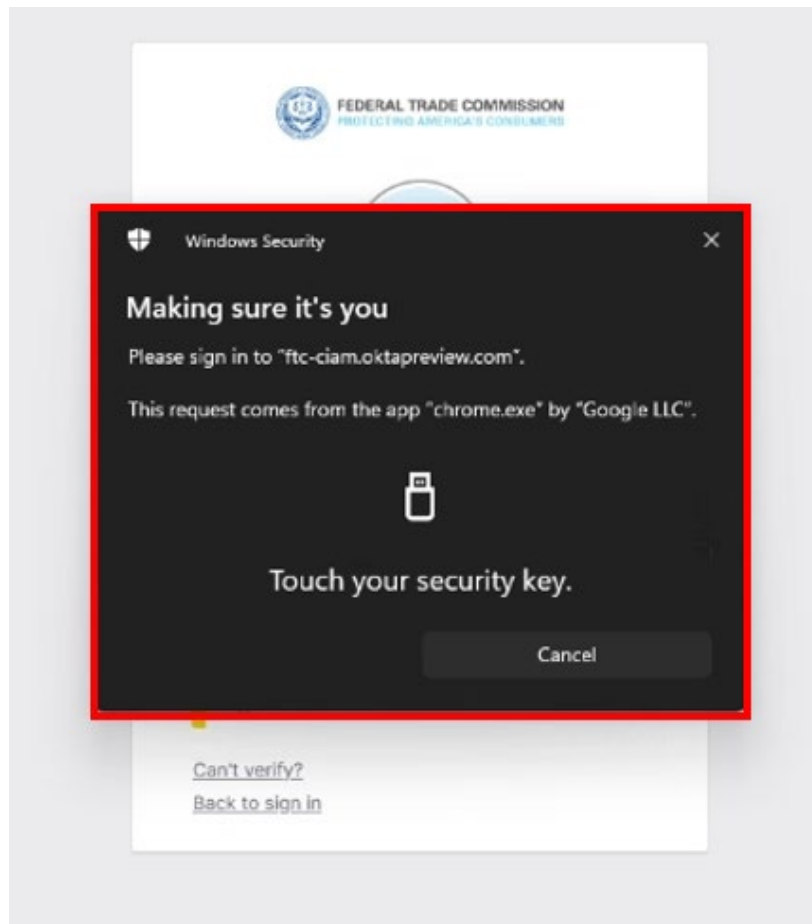
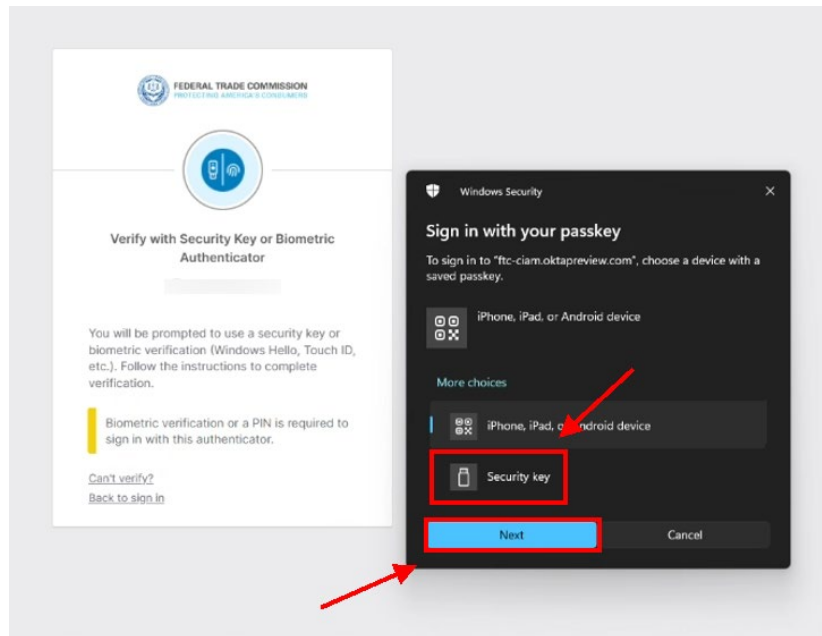


Your Passkey has now been saved, click “OK”.



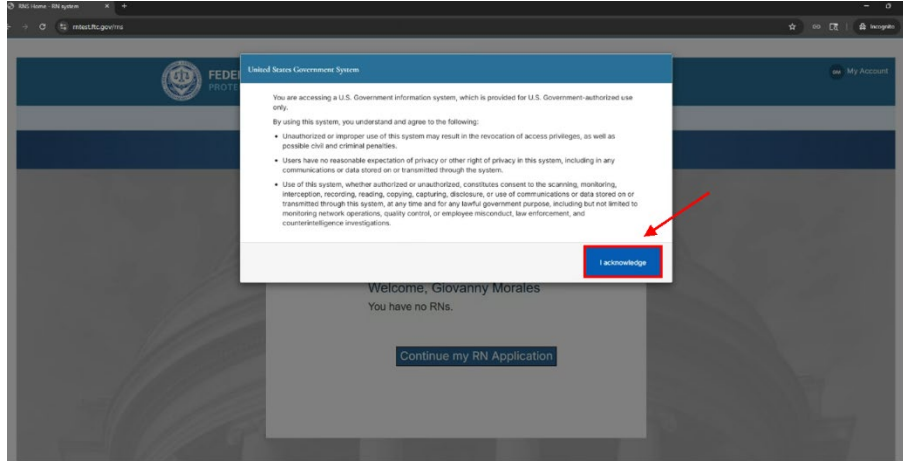
Now select “Continue” or configure another MFA factor if you choose, but not required.



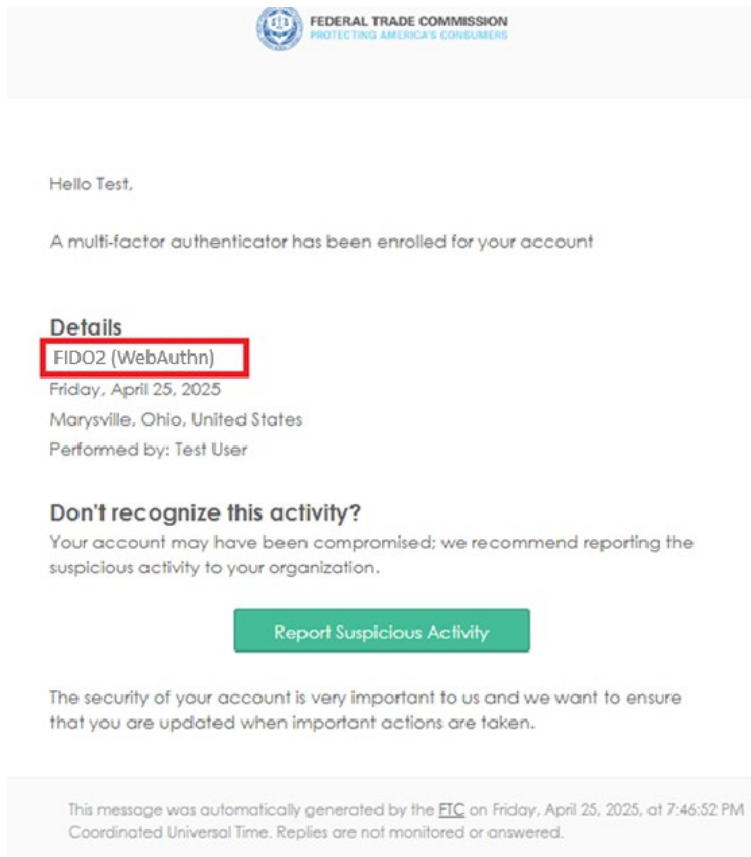


Step 3: Confirm and Save

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!

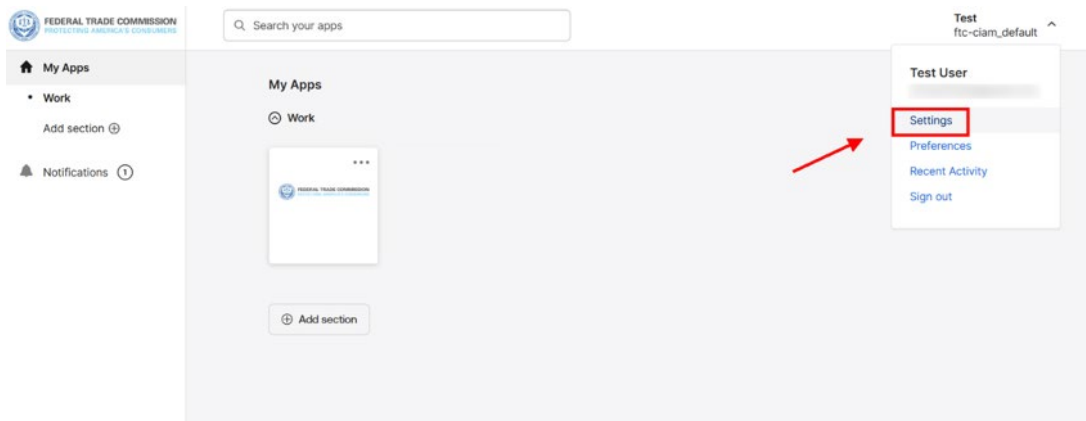
Your account registration with the FTC is now complete. You can now conveniently access all external FTC applications to which you have access through this account.

Note: *As an extra layer of security, once registered, you have 24 hours to submit a request for RN before your account will be deactivated. If you fail to submit a request within the 24 hour window and your account is locked, please contact RN_admin@ftc.gov.*

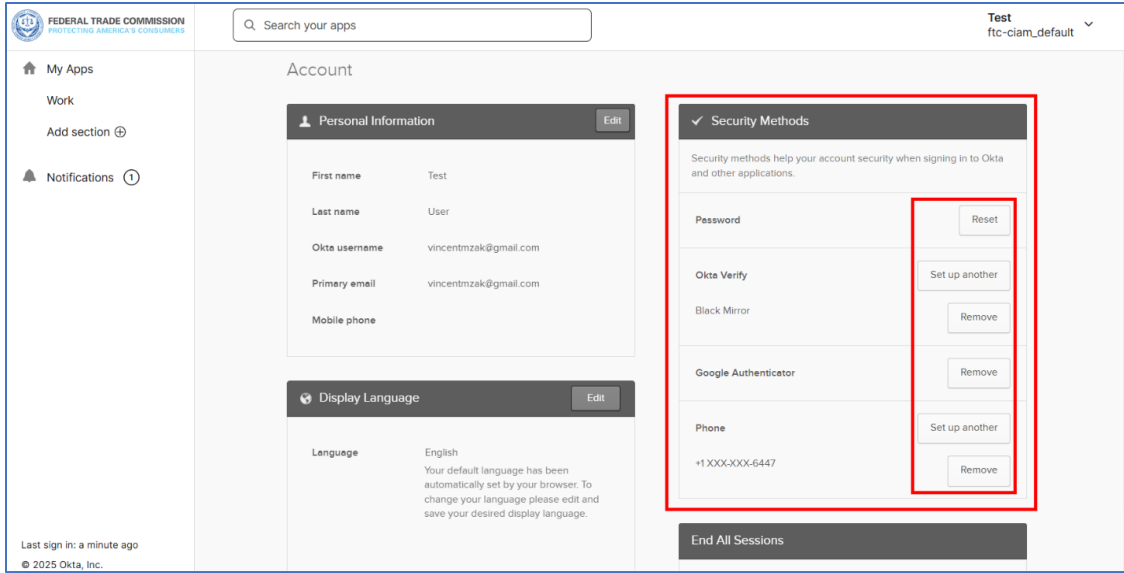
3.1.4 Updating Multi-Factor Authentication Settings

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

- 1) Navigate to: <https://ftc-ciam.okta.com/>
- 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.

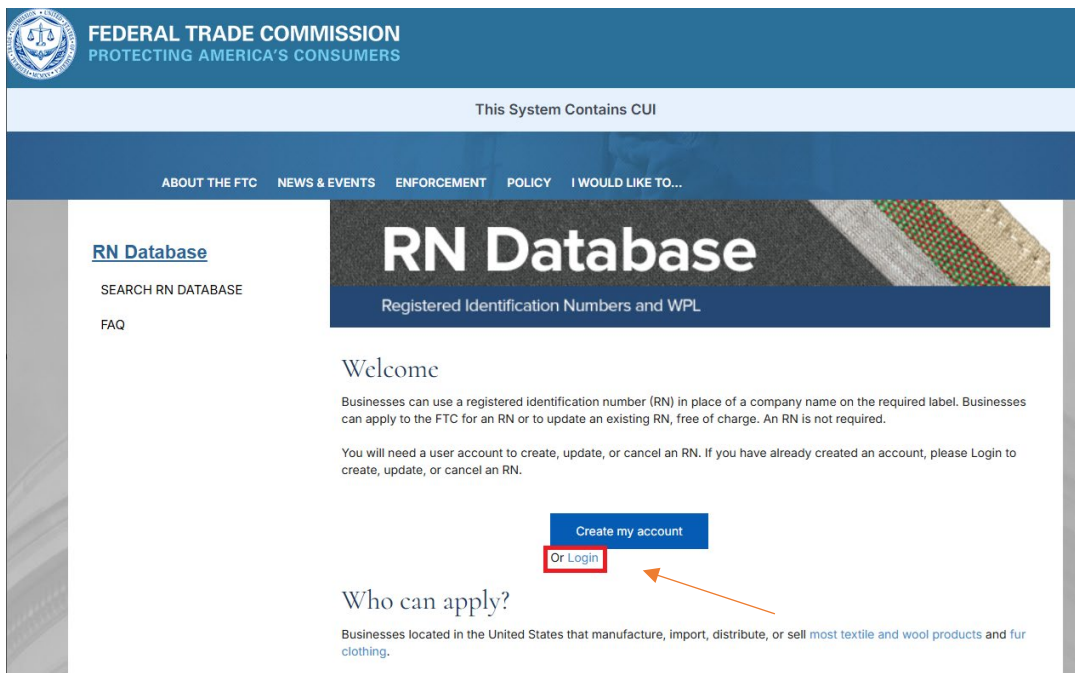


3.2 Registered Users

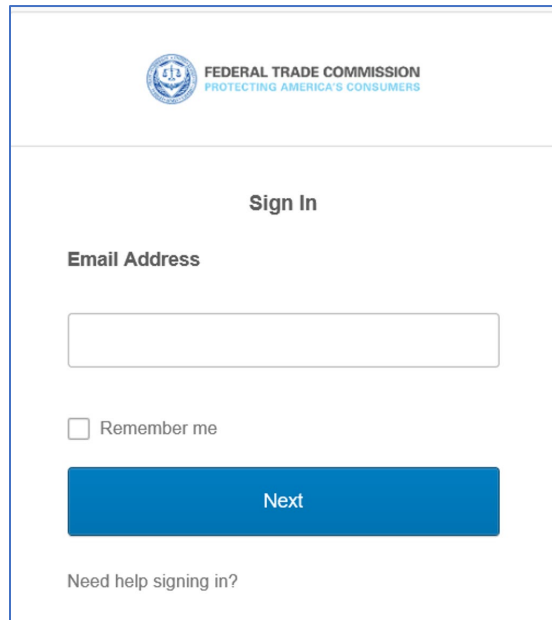
3.2.1 Login

If you have previously registered with the FTC, you can access the RN System by going to <https://rn.ftc.gov>.

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

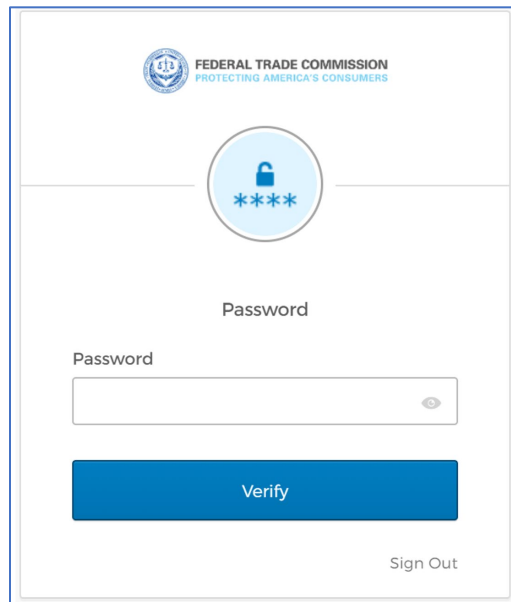


Enter your email address and click “Next”.



The image shows a web form for signing in. At the top left is the Federal Trade Commission logo with the text "FEDERAL TRADE COMMISSION" and "PROTECTING AMERICA'S CONSUMERS". Below the logo is the heading "Sign In". Underneath is the label "Email Address" followed by a text input field. Below the input field is a checkbox labeled "Remember me". At the bottom of the form is a blue button labeled "Next". Below the button is the text "Need help signing in?".

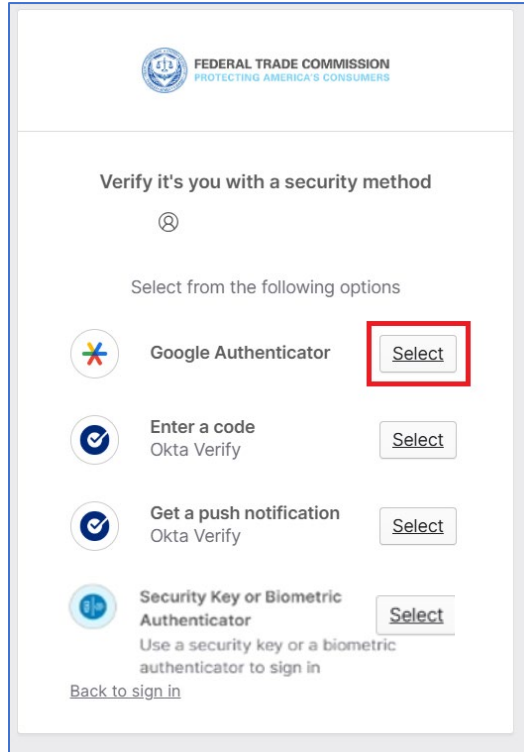
Then, enter in your password and click “Verify”.



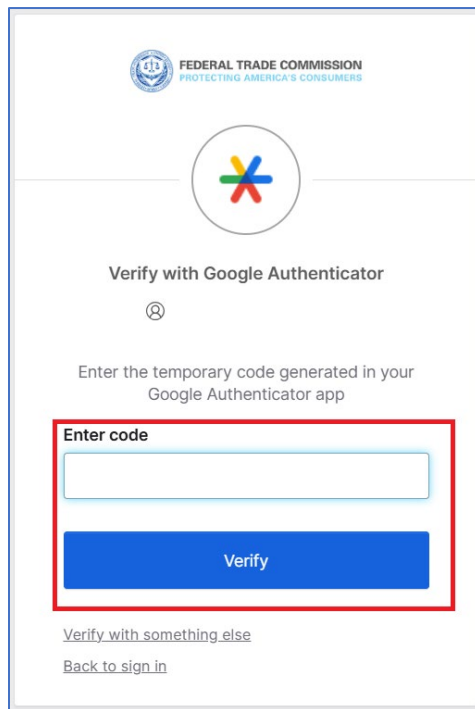
The image shows a web form for password verification. At the top left is the Federal Trade Commission logo with the text "FEDERAL TRADE COMMISSION" and "PROTECTING AMERICA'S CONSUMERS". Below the logo is a circular icon containing a padlock and the text "*****". Underneath is the label "Password". Below the label is the text "Password" followed by a password input field with a toggle eye icon. At the bottom of the form is a blue button labeled "Verify". Below the button is the text "Sign Out".

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

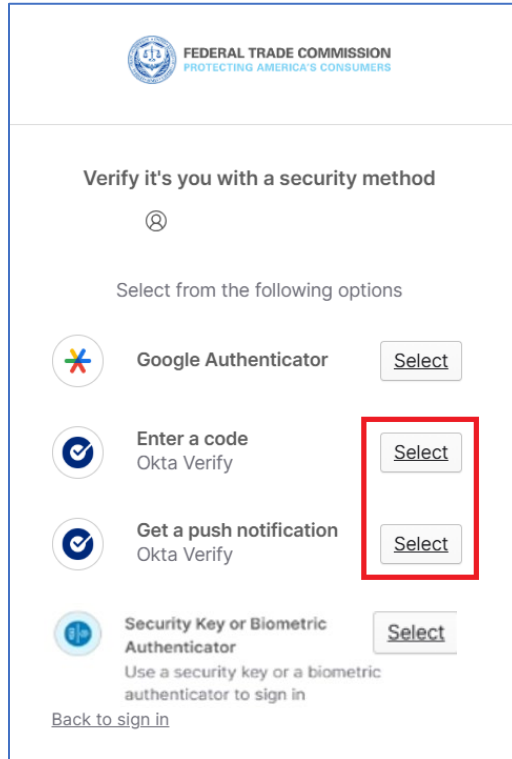
If you want to use “Google Authenticator” push “Select”.



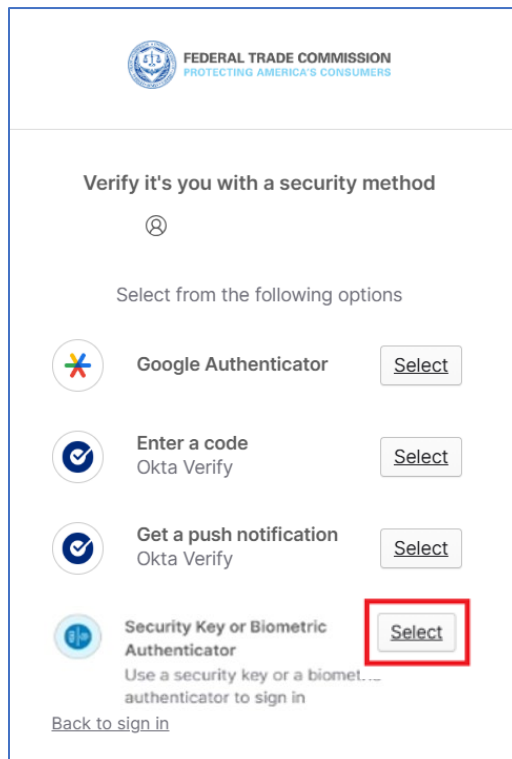
Now open Google Authenticator and enter the rolling One Time Password (OTP) and select “Verify”.



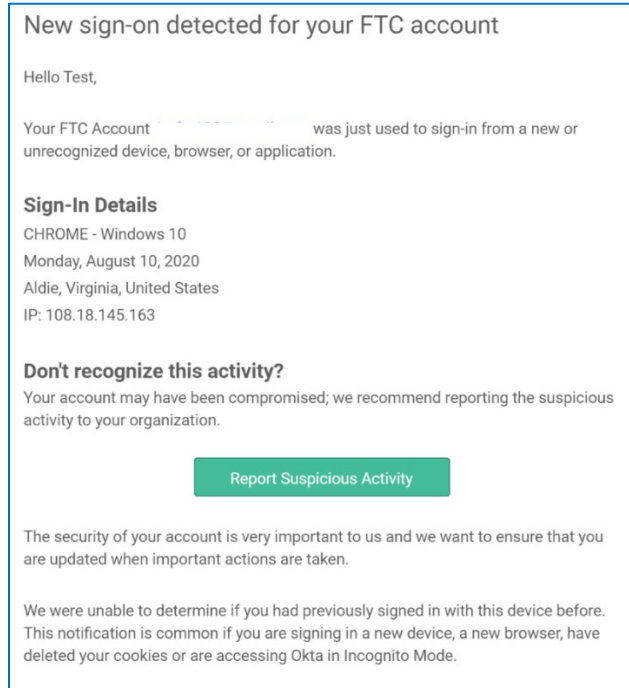
If want to use “Okta Verify,” select you “Enter a Code” or “Get a Push Notification”— **Push Notification is the suggested method**. Open your mobile device and push the prompt.



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

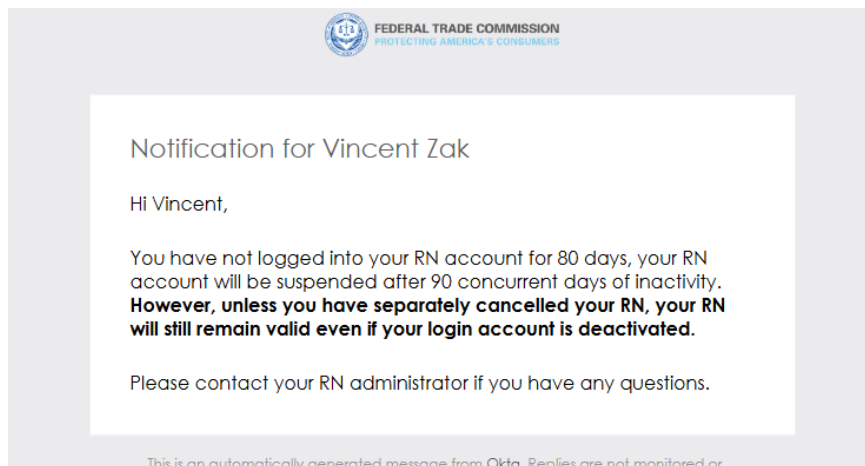


Upon successful authentication, you will be logged in to the application and you will receive an email notification confirming your login.



3.2.2 Reactivate Account

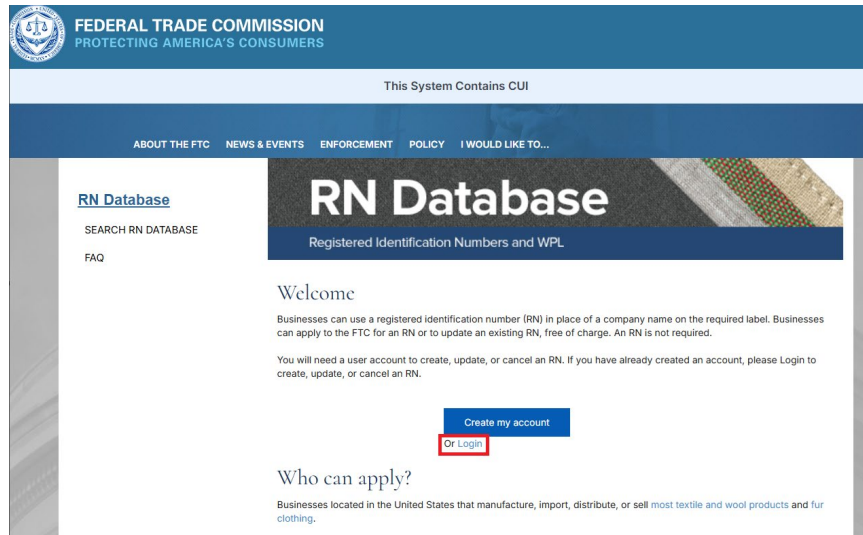
Your login account will be automatically deactivated after 90 days of inactivity. **However, unless you have separately cancelled your RN, your RN will still remain valid even if your login account is deactivated.** You will receive an email at 80 days of inactivity reminding that you should login again if you wish to keep your login account active before your account is deactivated after 90 days.



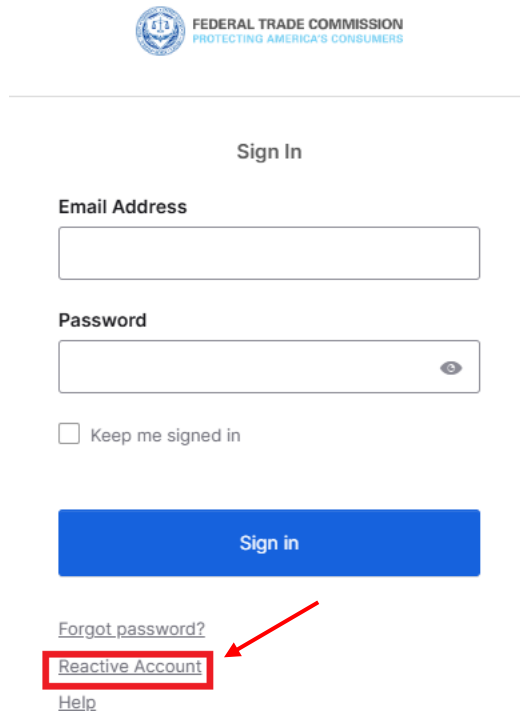
If you do not have activity in your account at 90 days, it will be automatically deactivated. You will not receive an email notification.

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

Navigate to <https://rn.ftc.gov> and click on the login button: You will be taken to the Okta RN System application sign on page. Now click “Login”.



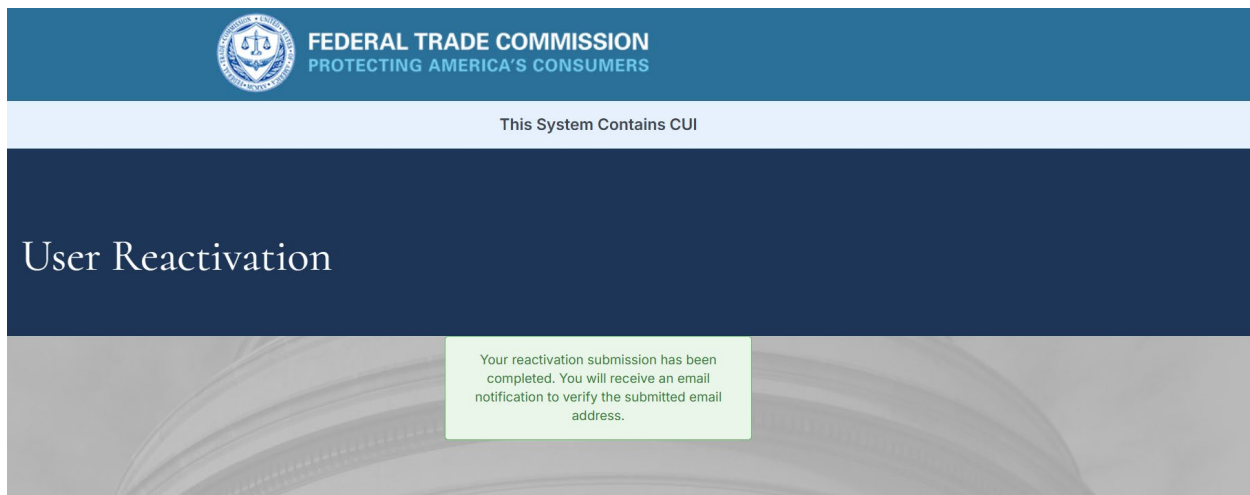
You will be rerouted to the Okta login page where you can select “Reactivate Account”.



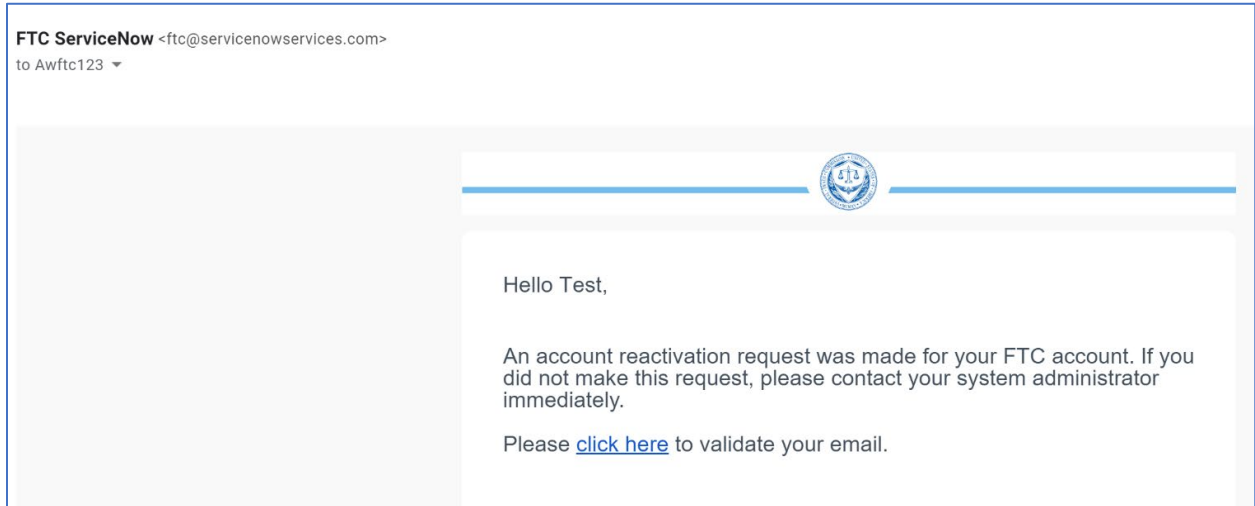
You will be taken to the RN System reactivation page. Enter your email address and click “Reactivate My Account”.



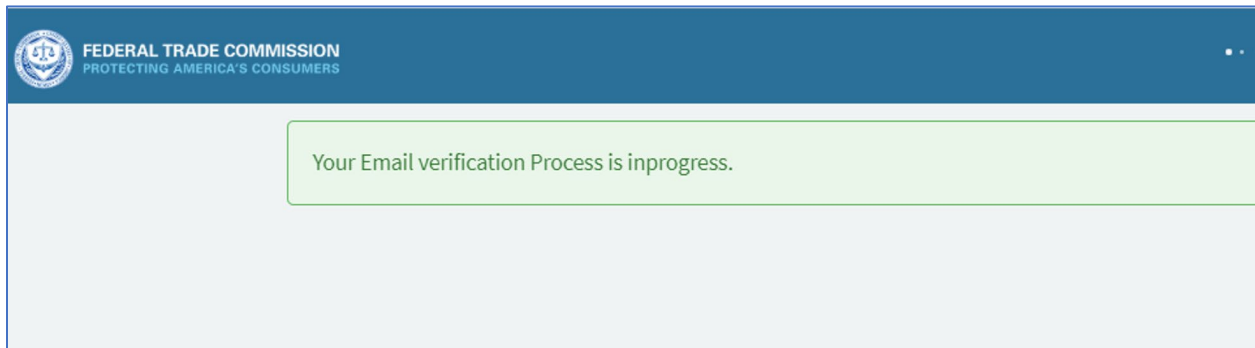
Upon entering your email address and clicking “Reactivate My Account,” you will receive the below on-screen confirmation, and you will also receive an email notification with a link to verify your account.



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

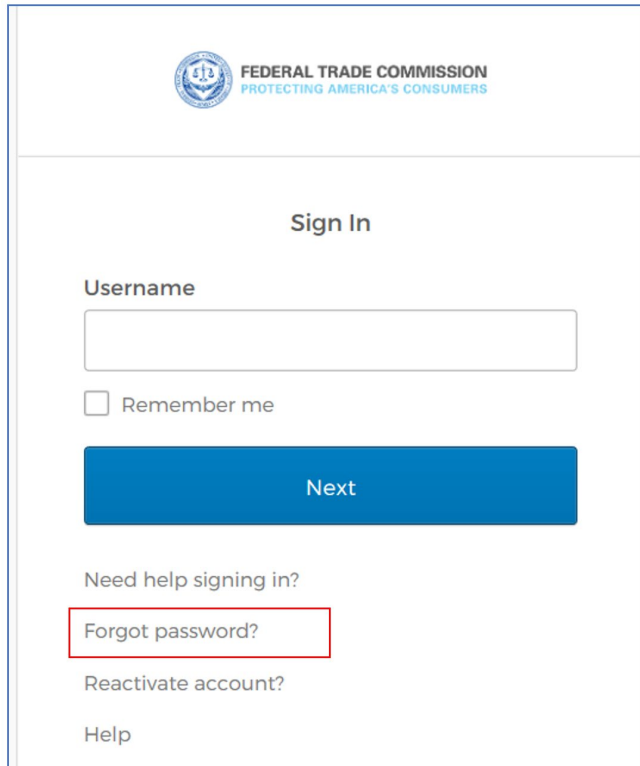


The following on-screen notification will be displayed confirming that your email verification is in progress. You will then receive another email confirming that your account has been successfully verified or if there was a problem with the verification.



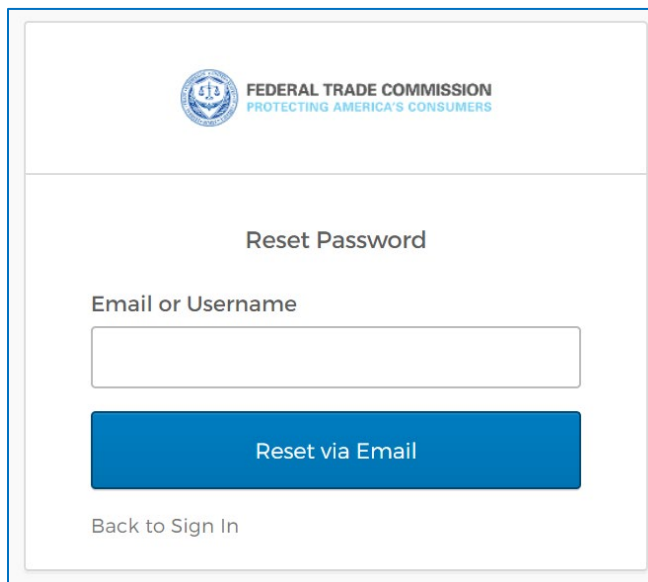
3.2.3 Reset Password

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



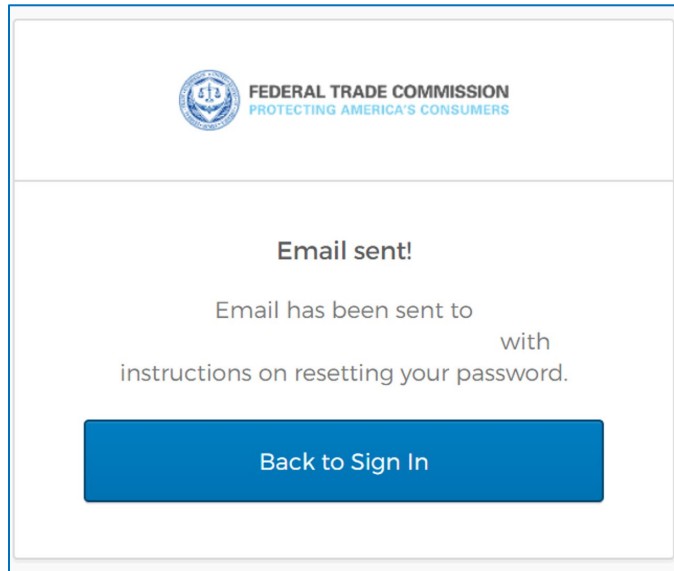
The screenshot shows the 'Sign In' page of the Federal Trade Commission system. At the top, there is the FTC logo and the text 'FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS'. Below this, the heading 'Sign In' is centered. There is a text input field for 'Username' and a checkbox labeled 'Remember me'. A blue button labeled 'Next' is positioned below the input fields. Underneath the 'Next' button, there are three links: 'Need help signing in?', 'Forgot password?' (which is highlighted with a red rectangular border), 'Reactivate account?', and 'Help'.

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

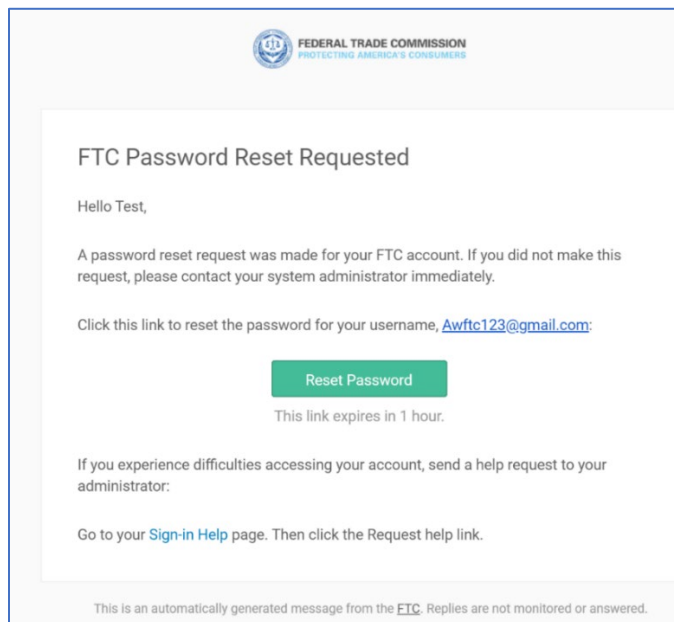


The screenshot shows the 'Reset Password' page of the Federal Trade Commission system. At the top, there is the FTC logo and the text 'FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS'. Below this, the heading 'Reset Password' is centered. There is a text input field for 'Email or Username'. A blue button labeled 'Reset via Email' is positioned below the input field. At the bottom left of the page, there is a link labeled 'Back to Sign In'.

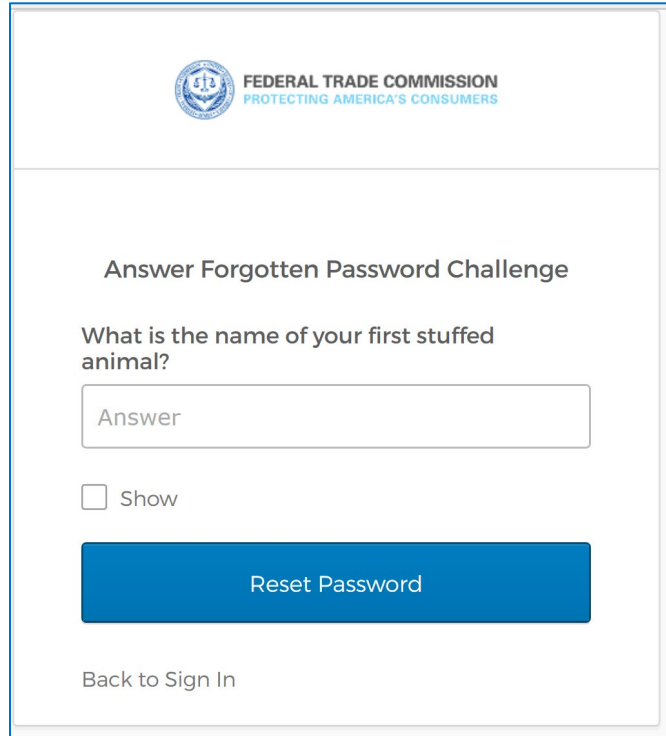
An on-screen confirmation will be displayed confirming that an email has been sent to your registered email account. Please open the email to proceed.



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

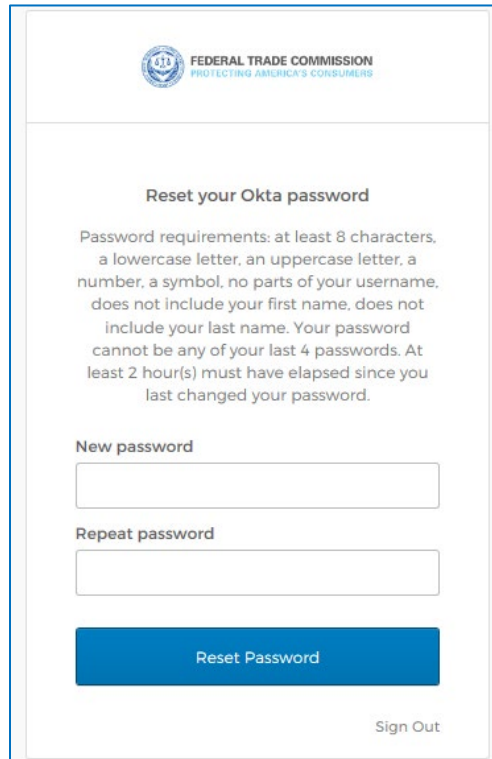


Upon clicking the link, you will be prompted to answer your security questions. Please enter in the answer and click “Reset Password”.



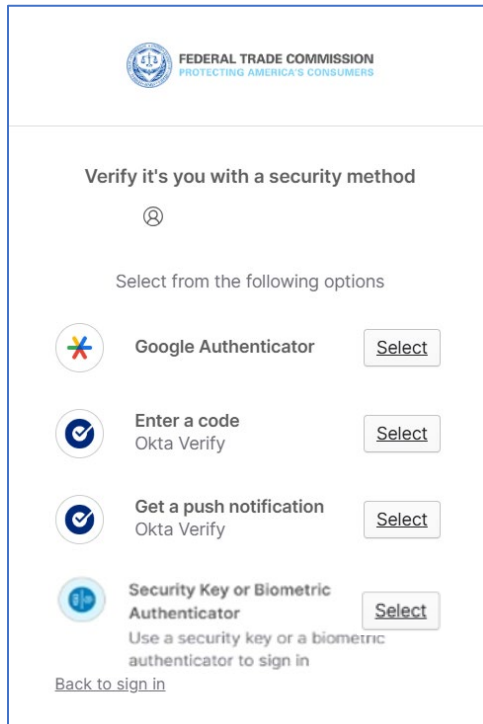
The screenshot shows a web form titled "Answer Forgotten Password Challenge" from the Federal Trade Commission. At the top left is the FTC logo with the text "FEDERAL TRADE COMMISSION" and "PROTECTING AMERICA'S CONSUMERS". The main heading is "Answer Forgotten Password Challenge". Below it is the question: "What is the name of your first stuffed animal?". There is a text input field with the placeholder text "Answer". Below the input field is a checkbox labeled "Show". At the bottom of the form is a large blue button labeled "Reset Password". Below the button is a link that says "Back to Sign In".

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



The screenshot shows a web form titled "Reset your Okta password" from the Federal Trade Commission. At the top left is the FTC logo with the text "FEDERAL TRADE COMMISSION" and "PROTECTING AMERICA'S CONSUMERS". The main heading is "Reset your Okta password". Below it is a paragraph of password requirements: "Password requirements: at least 8 characters, a lowercase letter, an uppercase letter, a number, a symbol, no parts of your username, does not include your first name, does not include your last name. Your password cannot be any of your last 4 passwords. At least 2 hour(s) must have elapsed since you last changed your password." Below the requirements are two text input fields: "New password" and "Repeat password". At the bottom of the form is a large blue button labeled "Reset Password". Below the button is a link that says "Sign Out".

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



4. Login to RN System

To log into the RN system, navigate to <https://rn.ftc.gov/rns>.

5. Troubleshooting

If you need further assistance setting up Multi-Factor Authentication or have questions that are technical in nature, please contact support.rnsystem@ftc.gov. If you need further assistance with other issues relating to RNs, please contact rn_admin@ftc.gov.