



INFORMATION SECURITY

Profile Manager Quick Reference Guide

Published 09/02/2025

Member FDIC



Table of Contents

Overview	3
New User Activation	3
Profile Manager Login Methods	5
First Method:	5
Second Method:	7
Welcome Message	8
Profile Manager Pages	8
Profile Info	9
Security	11
Okta Verify Enrollment	13
Google Authenticator Enrollment	16
Text Message Authentication (SMS) Enrollment	20
Voice Call Authentication Enrollment	23
Additional Information for Remove and Reset Options:	26
Single Sign-On	29

This document is intended to operate as a guide to facilitate the easy use of the products it discusses. It does not and is not intended to alter, modify, waive, or change any agreements between users of the product and First Citizens Bank & Trust Co., or any terms and conditions imposed by First Citizens Bank & Trust Co. for use of the product. In the event that there is any conflict between this document and any applicable agreements or terms and conditions imposed by First Citizens Bank & Trust Co., those applicable agreements or terms and conditions shall control.

Overview

The Profile Manager application is a self-service application where customers can update the following information:

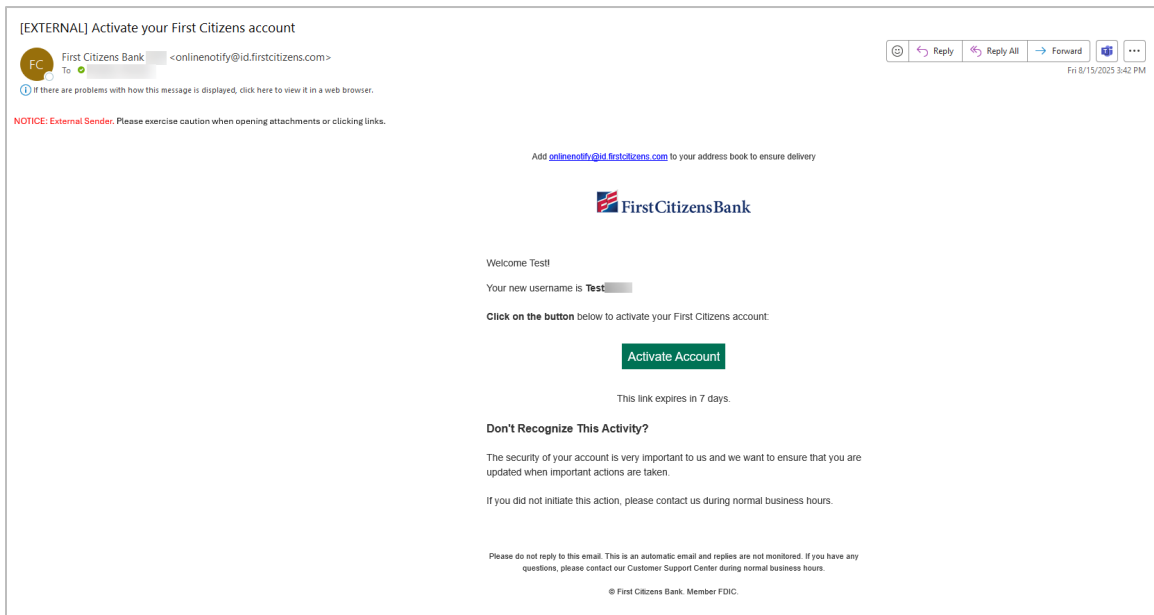
- First Name
- Last Name
- Email
- Mobile Number
- Multi-Factor Authentication Factor
- Activate Single Sign On (SSO) to log into one or more applications with the same credentials

New User Activation

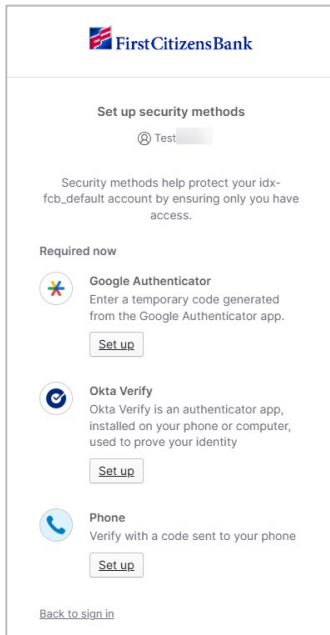
As a prerequisite to utilizing Profile Manager, the following new user activation process will take place. When a new user is created, they will receive an activation email.

Note: If you've already completed the new user activation process, you can skip this section.

1. Select the **Activate Account** button to activate the account and establish your preferred MFA method.

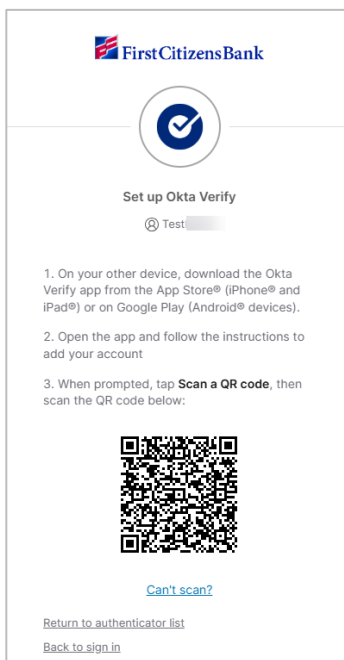


2. Set up one of the available methods of verification.



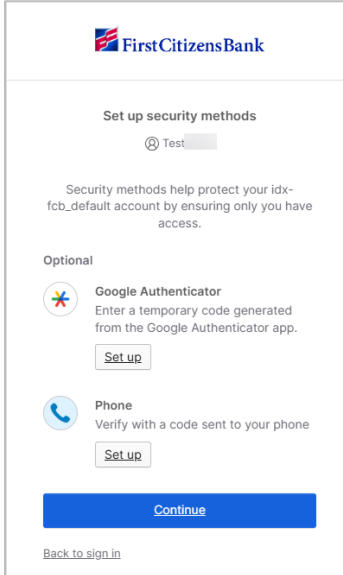
3. Once verification method is selected, you will be prompted with a screen like the one below.

Note: The below is a sample for **Okta Verify** authentication method. Other methods of verification are detailed further in the guide.



4. Once a method has been set up, the established factor will no longer display on the setup page when you log in.

Note: As shown below, **Okta Verify** is not listed on the setup page.



First Citizens Bank

Set up security methods

Test

Security methods help protect your idx-fcb_default account by ensuring only you have access.

Optional

Google Authenticator
Enter a temporary code generated from the Google Authenticator app.
[Set up](#)

Phone
Verify with a code sent to your phone
[Set up](#)

[Continue](#)

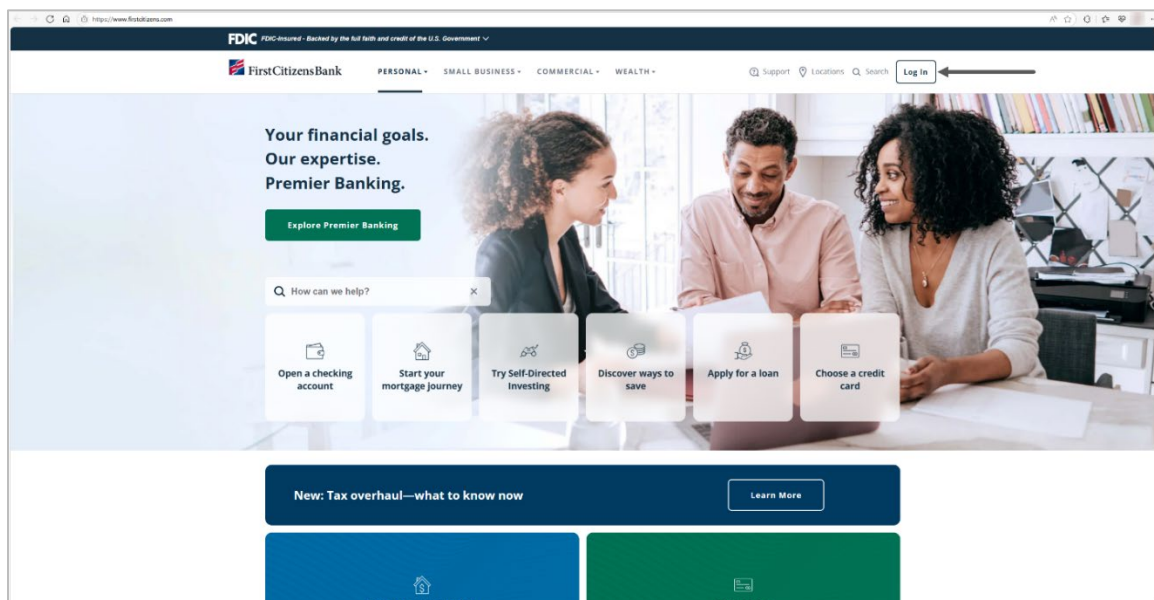
[Back to sign in](#)

Profile Manager Login Methods

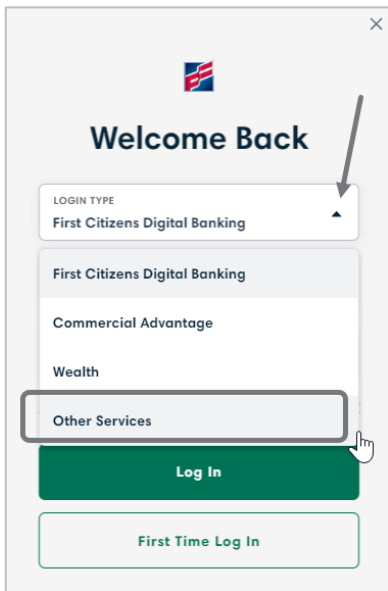
There are several methods to log into Profile Manager:

First Method:

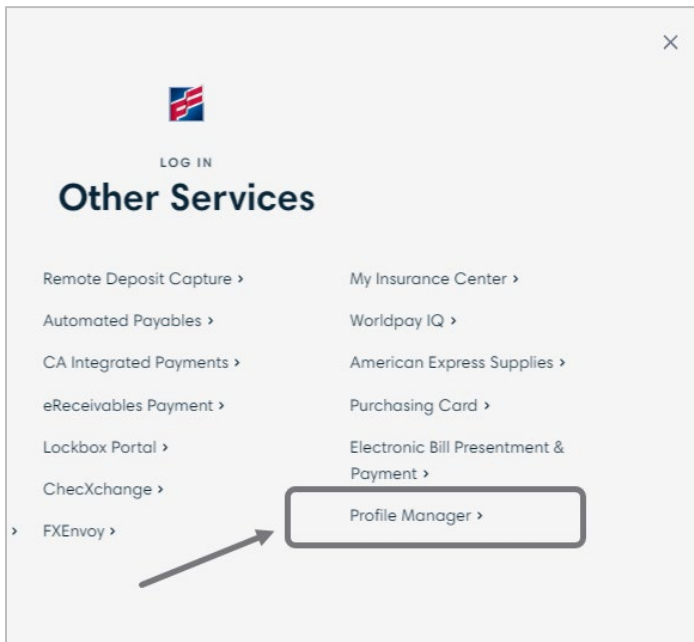
1. Navigate to www.firstcitizens.com home page, click on the **Log In** button at the top right-hand corner.



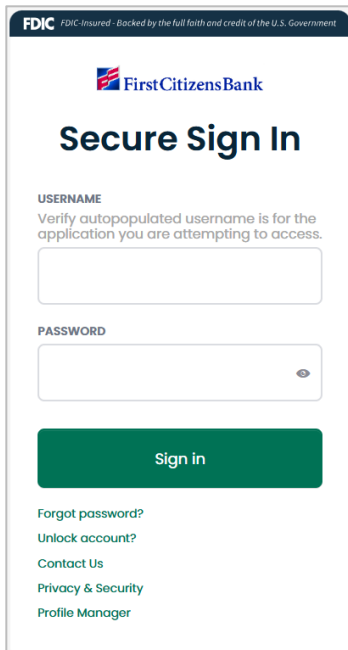
- You will be directed to the **Welcome Back** page. Select the drop-down caret, then select **Other Services** from the list of options.




- Find the **Profile Manager** hyperlink under **Other Services**. Click on the **Profile Manager** link.



4. Log in using your credentials.



FDIC FDIC-Insured - Backed by the full faith and credit of the U.S. Government

 **First Citizens Bank**

Secure Sign In

USERNAME
Verify autopopulated username is for the application you are attempting to access.

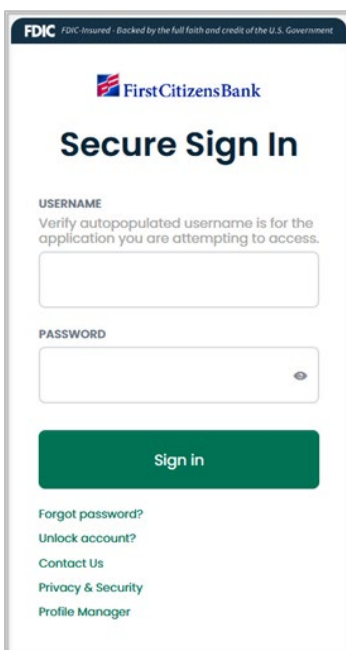
PASSWORD

Sign in


[Forgot password?](#)
[Unlock account?](#)
[Contact Us](#)
[Privacy & Security](#)
[Profile Manager](#)

Second Method:

1. Navigate to the link <https://profile.firstcitizens.com/>.
2. Log in using your credentials.



FDIC FDIC-Insured - Backed by the full faith and credit of the U.S. Government

 **First Citizens Bank**

Secure Sign In

USERNAME
Verify autopopulated username is for the application you are attempting to access.

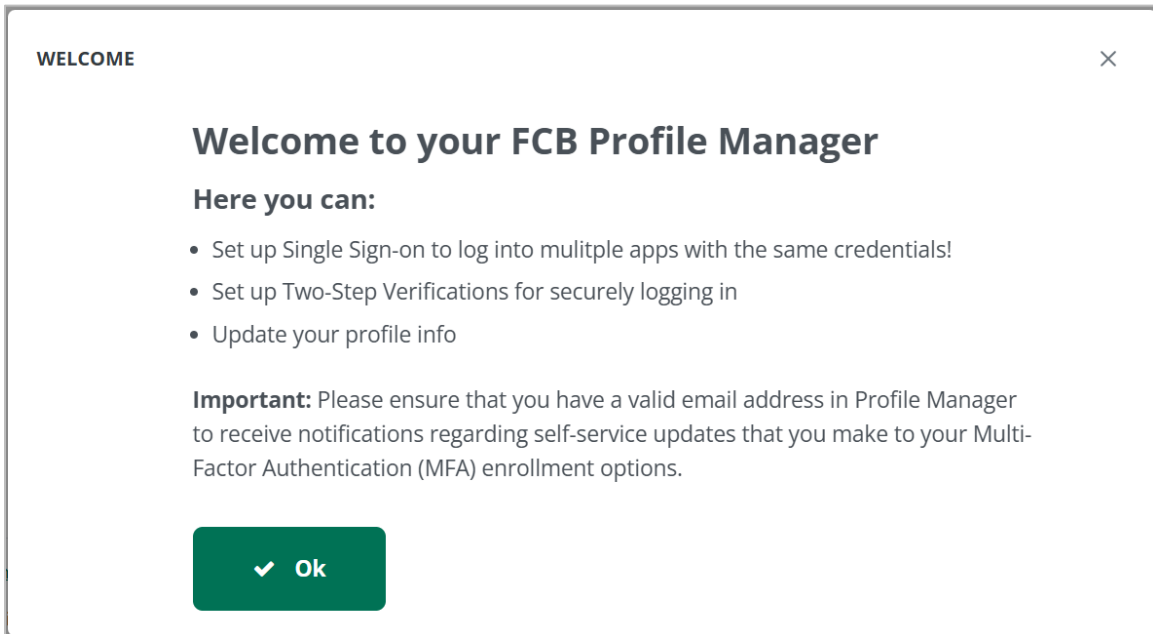
PASSWORD

Sign in

[Forgot password?](#)
[Unlock account?](#)
[Contact Us](#)
[Privacy & Security](#)
[Profile Manager](#)

Welcome Message

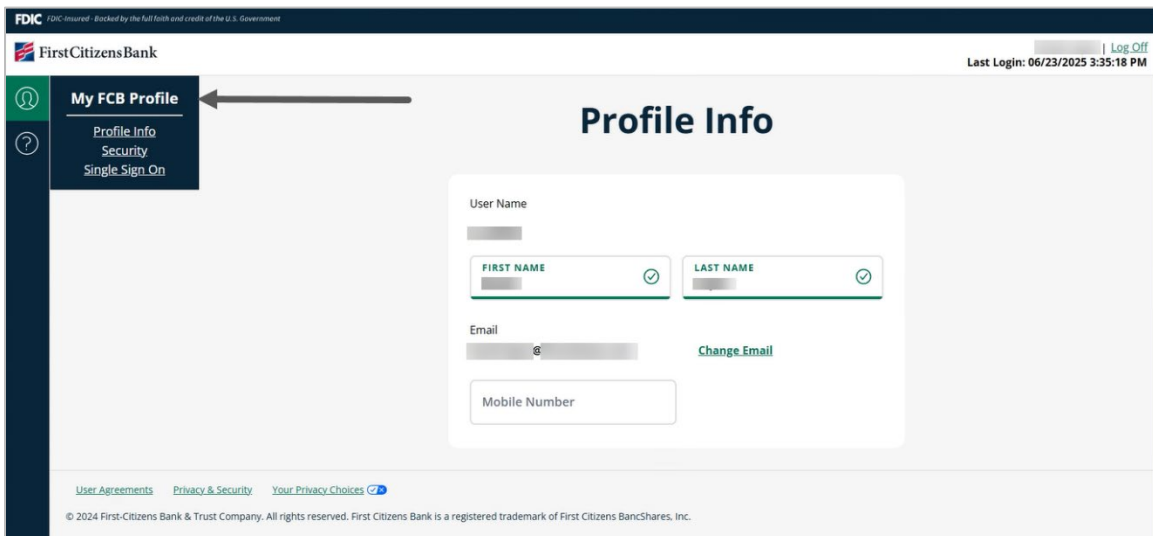
When you access Profile Manager for the first time, a window will open with a welcome message. Select the **Ok** button or click on the **X** on the top-right corner to continue your session.



Profile Manager Pages

There are three tabs (or pages) in Profile Manager:

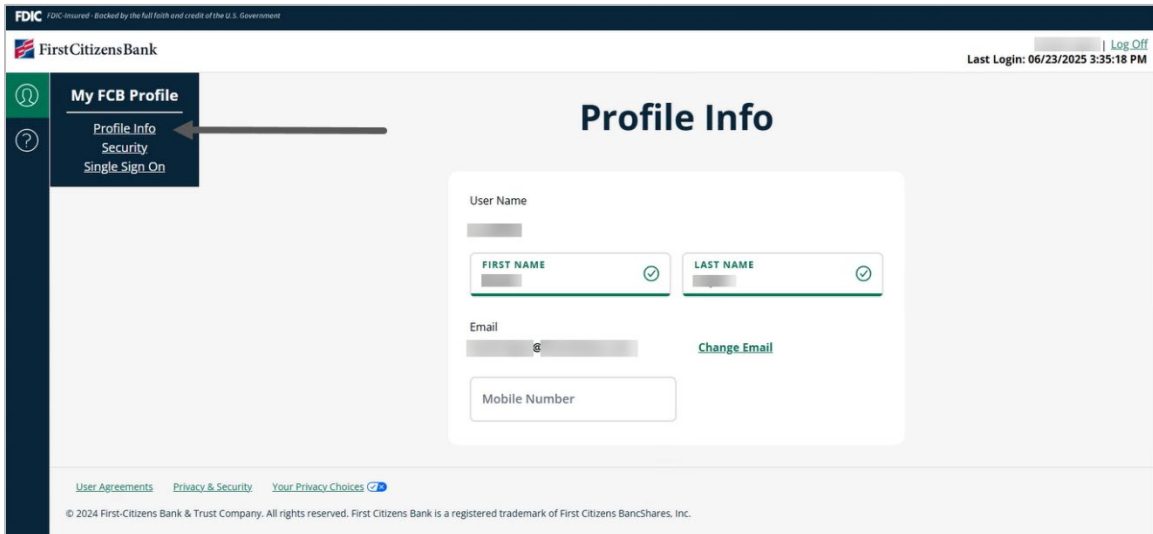
- Profile Info
- Security
- Single Sign On



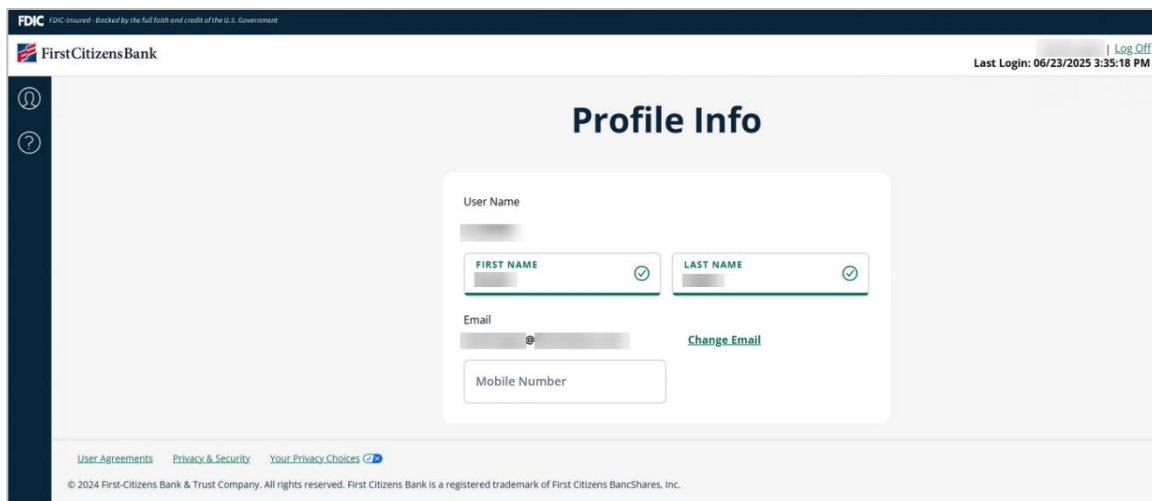
Profile Info

You can self-service **First Name**, **Last Name**, **Email**, and **Mobile Number**.

Note: **User Name** is not an editable field.

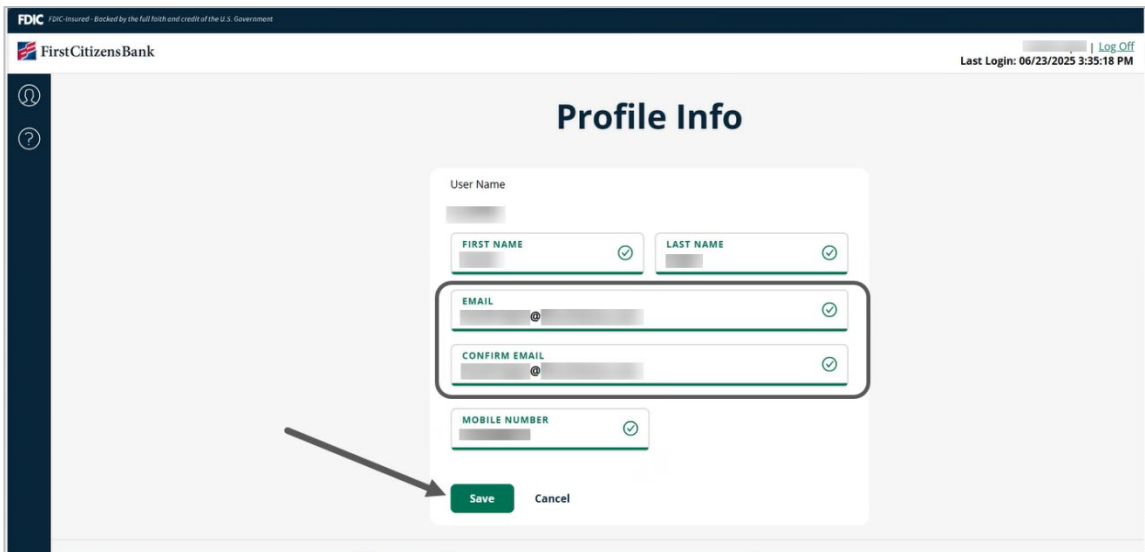


- To update first name, click on the blank space under the field name and above the line, make the necessary change and tab to the next field. **First Name Successfully Updated** success message will display.
- To update last name, click on the blank space under the field name and above the line, make the necessary change and tab to the next field. **Last Name Successfully Updated** success message will display.



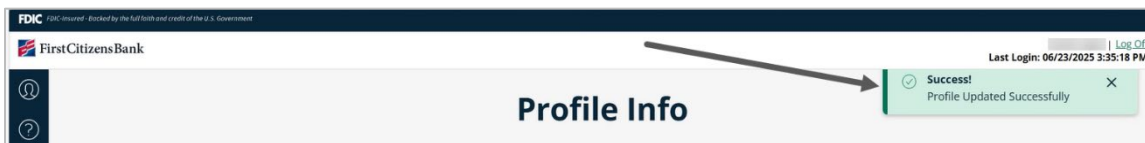
- The email address used while creating a profile is shown as not editable next to the **Change Email** link. To update the email address, you must click on the **Change Email** link. Enter the new email address in the **Email*** field. Re-enter the same email address on the **Confirm*** email. Click on **Save**.

Note: The email address must be in [abc@xyz.com](#) format.



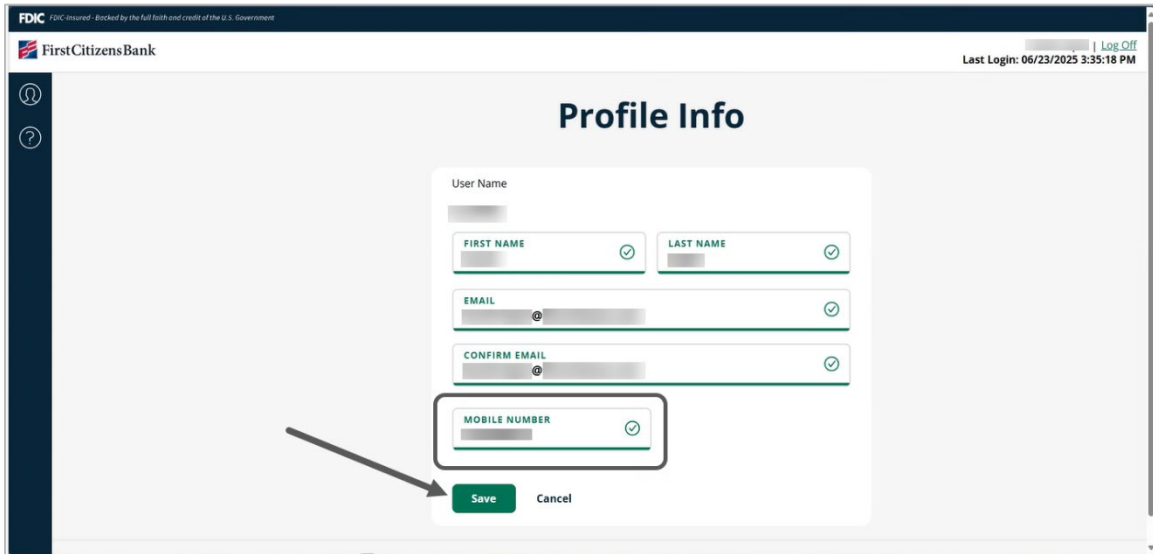
The screenshot shows the 'Profile Info' page in the First Citizens Bank system. The page header includes 'FDIC' and 'First Citizens Bank' logos, along with a 'Log Off' link and the text 'Last Login: 06/23/2025 3:35:18 PM'. The main content area is titled 'Profile Info' and contains a form with the following fields: 'User Name', 'FIRST NAME', 'LAST NAME', 'EMAIL', 'CONFIRM EMAIL', and 'MOBILE NUMBER'. Each field has a checkmark icon to its right. The 'EMAIL' and 'CONFIRM EMAIL' fields are highlighted with a red box. A red arrow points to the 'Save' button at the bottom of the form.

- **Email Successfully Updated** success message will display.



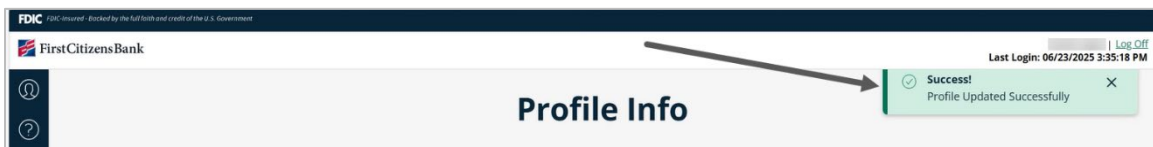
The screenshot shows the 'Profile Info' page after the email has been updated. The page header is the same as in the previous screenshot. The main content area is titled 'Profile Info'. A green success message box is displayed in the top right corner, containing a checkmark icon, the text 'Success!', and 'Profile Updated Successfully'. A red arrow points to the success message box.

- To add or update **Mobile Number**, click on the blank space under the field name, make the necessary change, then click on **Save**.



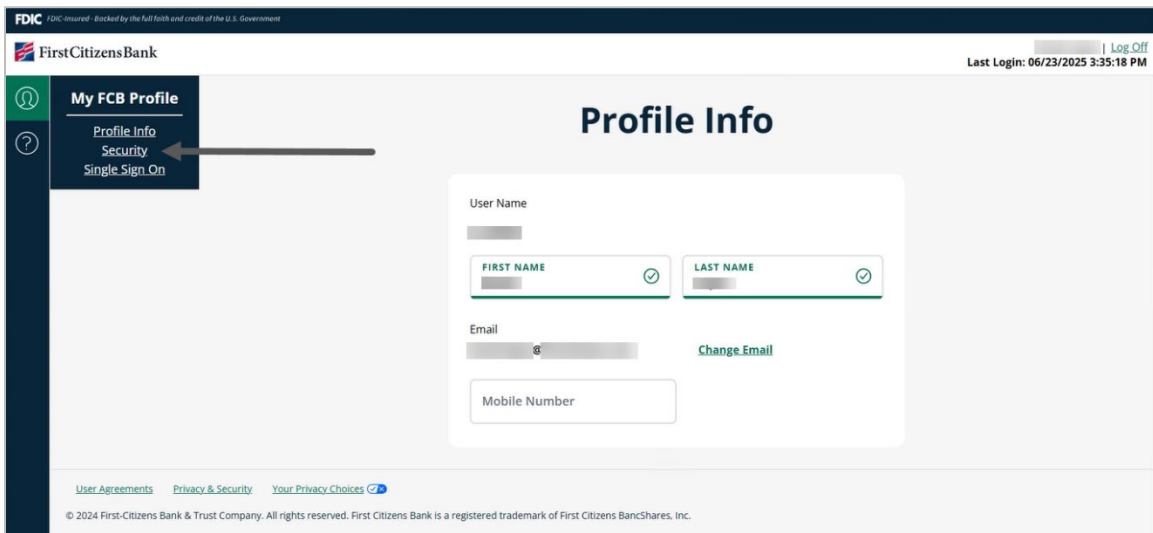
The screenshot shows the 'Profile Info' page in the First Citizens Bank user interface. The form contains the following fields: 'User Name' (with sub-fields for 'FIRST NAME' and 'LAST NAME'), 'EMAIL', 'CONFIRM EMAIL', and 'MOBILE NUMBER'. Each field has a green checkmark icon to its right, indicating it is valid. A red box highlights the 'MOBILE NUMBER' field, and a red arrow points from it to the 'Save' button at the bottom of the form. The 'Save' button is green, and the 'Cancel' button is grey.

- Profile Updated Successfully** success message will display.

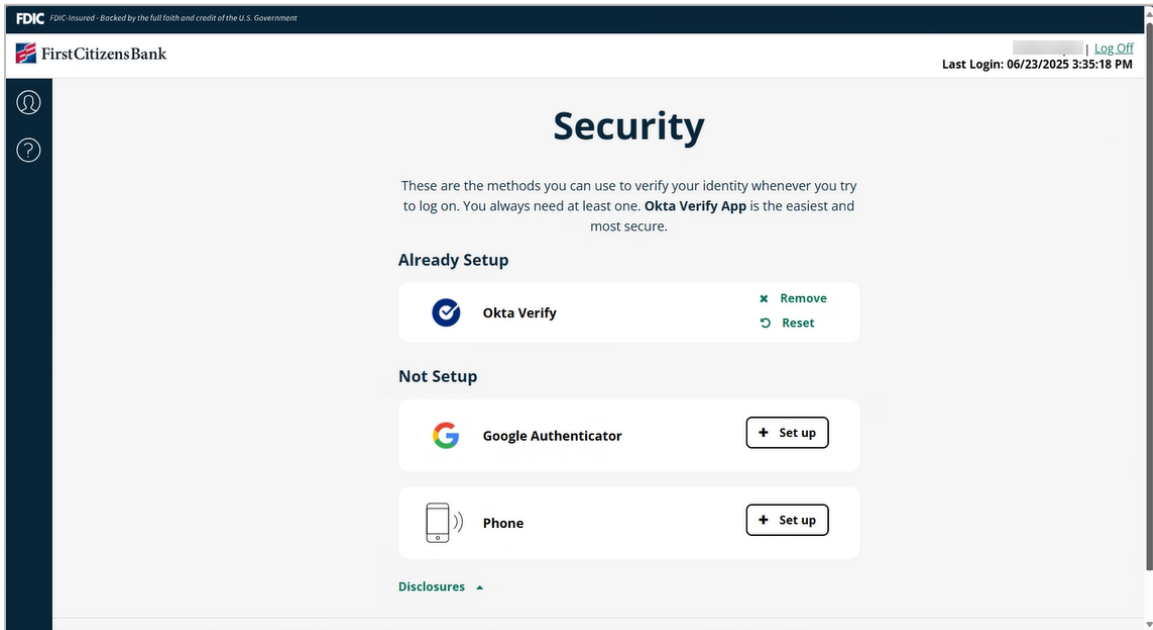


Security

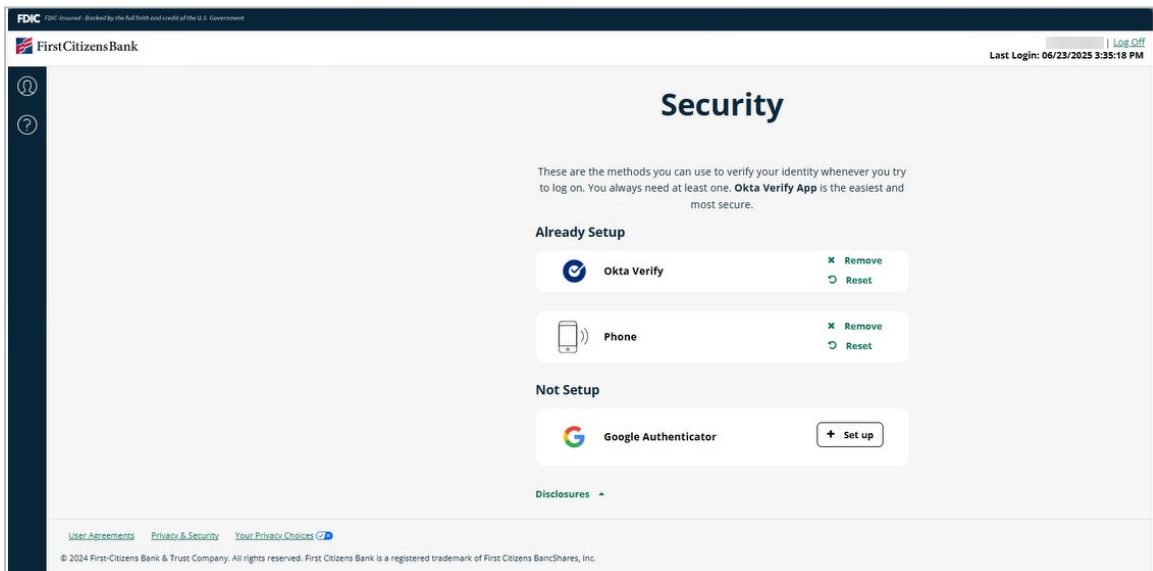
- You can enroll in Multi Factor Authentication (MFA) method by navigating to the **Security** page.



2. Select **+ Set up** button to enroll in a new MFA option. You can also **Remove** or **Reset** an established method.



3. NEW MFA users will have three options available; we recommend registering for more than one MFA.



Okta Verify

- Uses a push notification sent to the mobile app (requires application download).

Google Authenticator

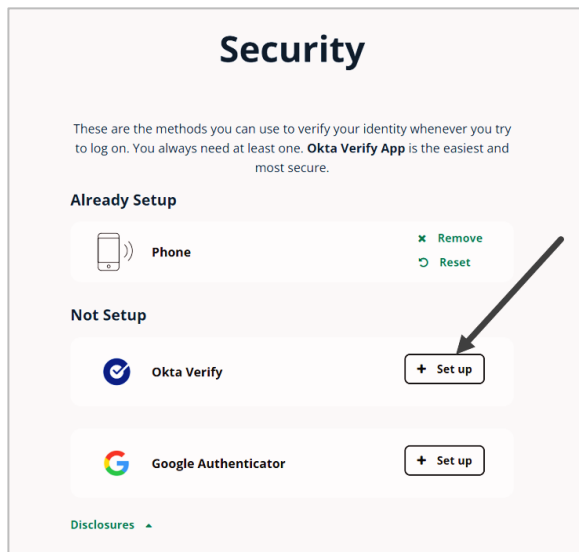
- Enter a single-use code from the mobile app (requires application download).

Phone Authenticator

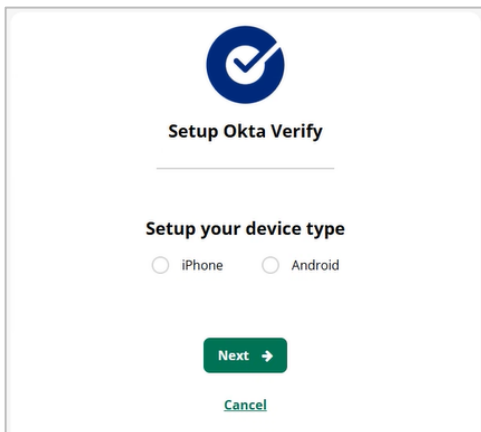
- Enter a single-use code sent to your mobile phone via text **OR** via phone call.

Okta Verify Enrollment

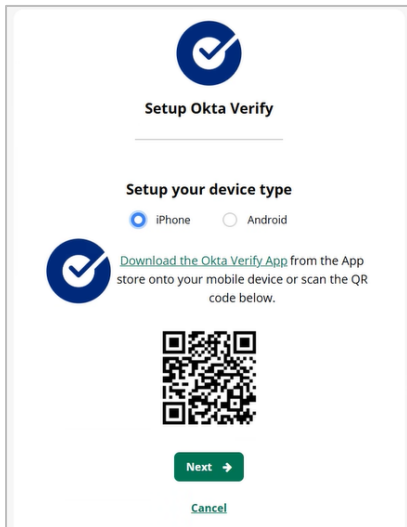
1. Click **+Set up** next to Okta Verify.



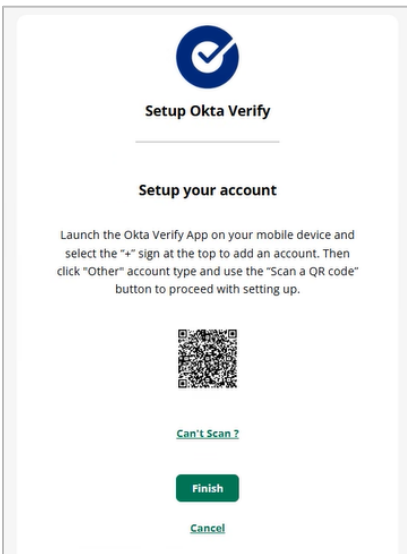
2. Select your device type.



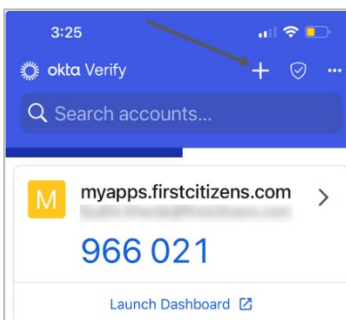
3. Download **Okta Verify** app from Apple App Store (iPhone) or Google Playstore (Android) first, then click **Next**.



4. Launch **Okta Verify** app on your mobile device.



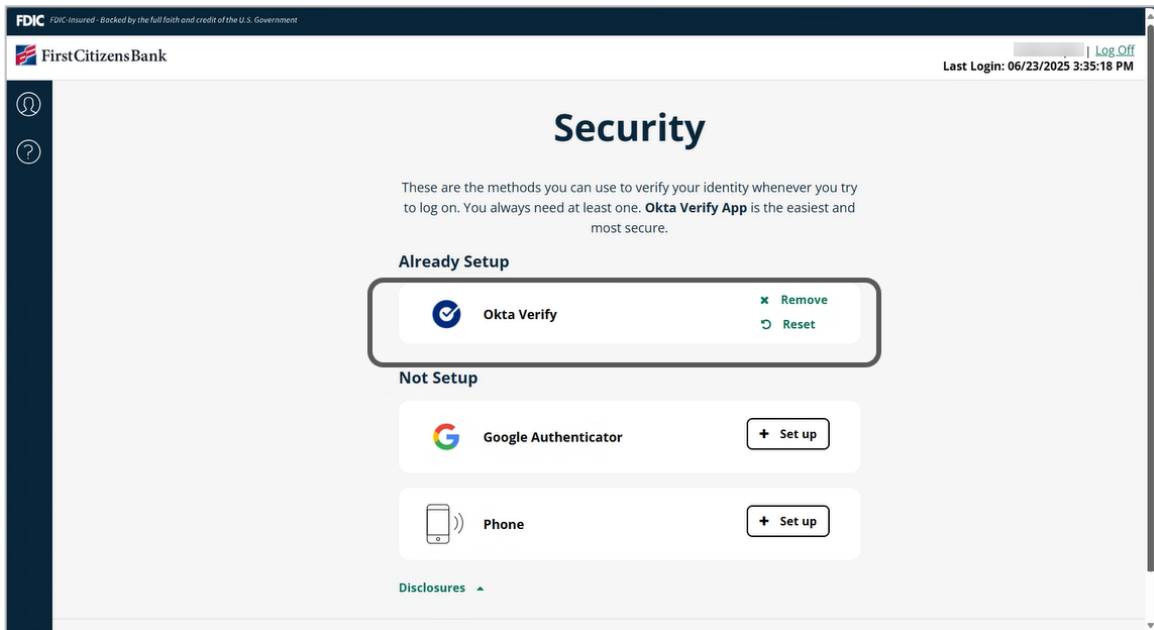
5. Select **+** icon to add an account.



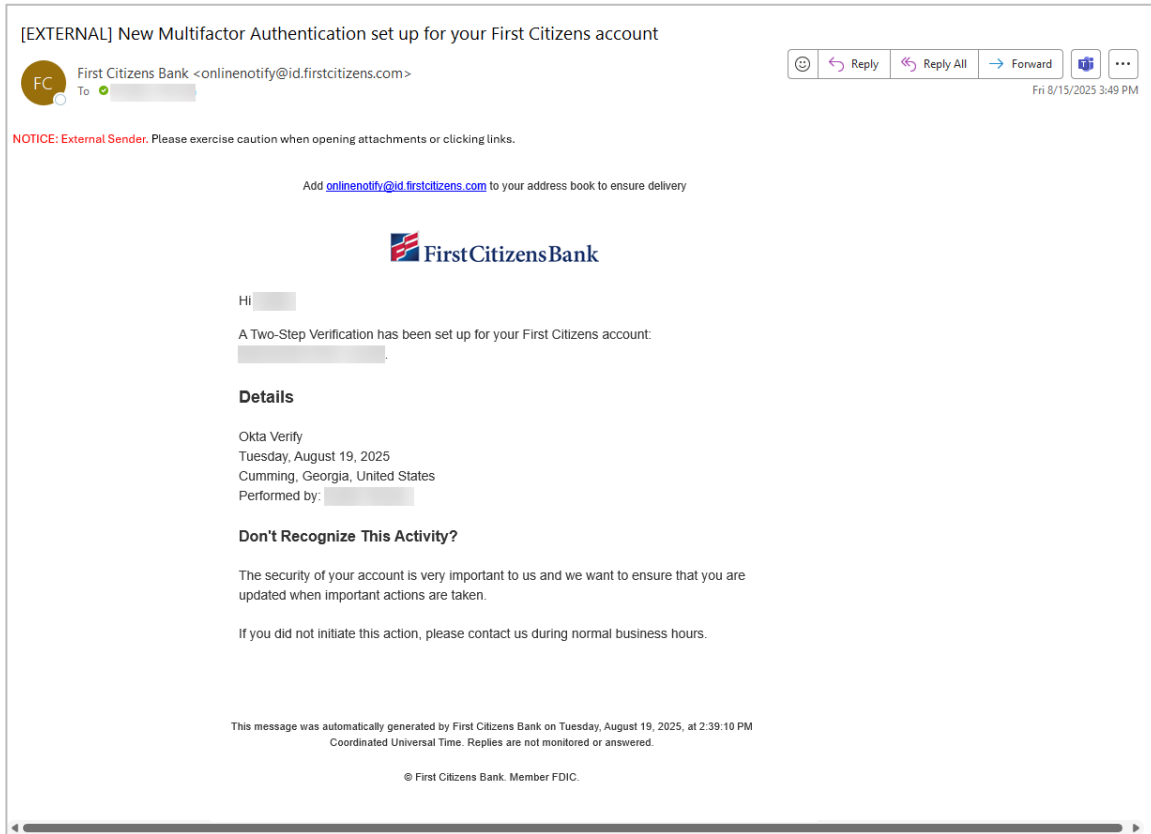
6. Scan the QR code using your mobile device.

Note: If you do not wish to allow access to your mobile device camera, click the **Can't scan?** link and follow the instructions provided in the FAQ.

7. **Success 2 step verification complete** success message will display.
8. The **Okta Verify** factor will display in the **Already Setup** queue. The **+ Set up** button will be replaced with a **Remove** and a **Reset** button.

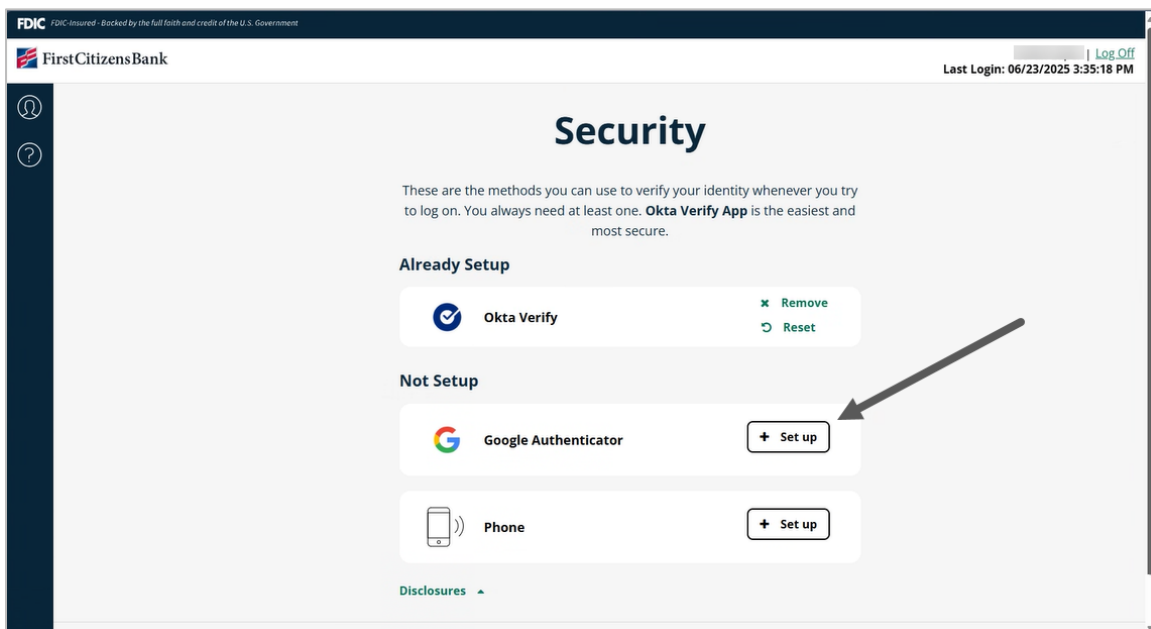


9. You will receive an email confirming that a multifactor authenticator has been set up.

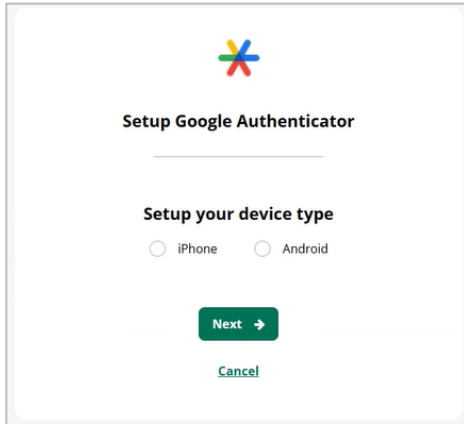


Google Authenticator Enrollment

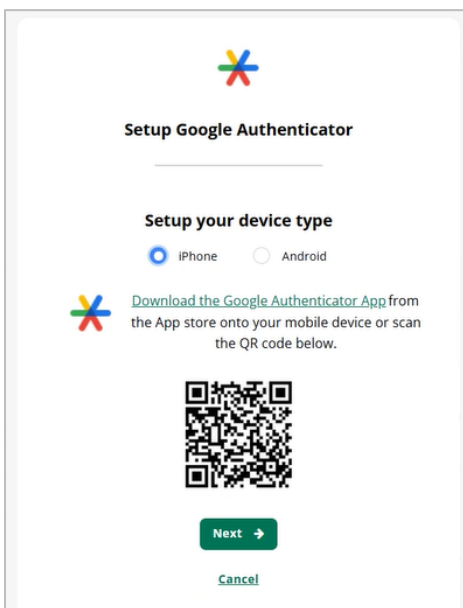
1. Click + **Set up** next to Google Authenticator.



2. Select your device type.



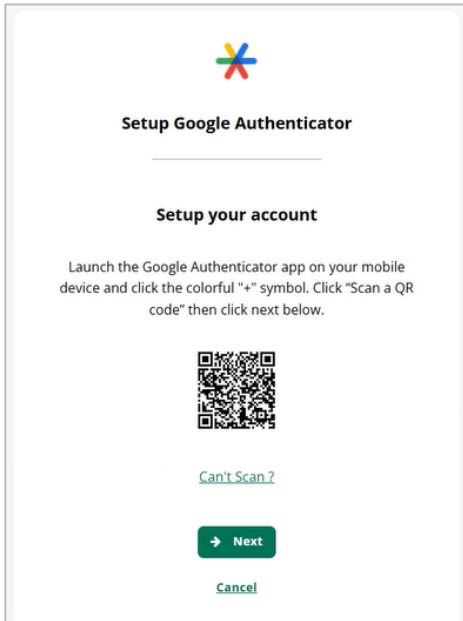
3. Download the Google Authenticator App from the App Store (iPhone) or Google Playstore (Android) first, then click **Next**.



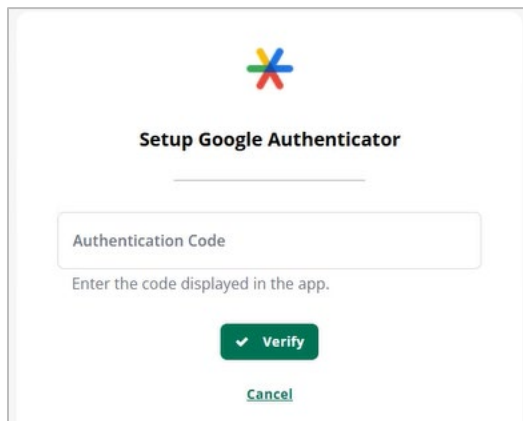
4. Launch Google Authenticator app on your mobile device and tap the + icon.

5. Scan the QR code using your mobile device.

Note: If you do not wish to allow access to your mobile device camera, click the **Can't scan?** link and follow the instructions provided in the FAQ.

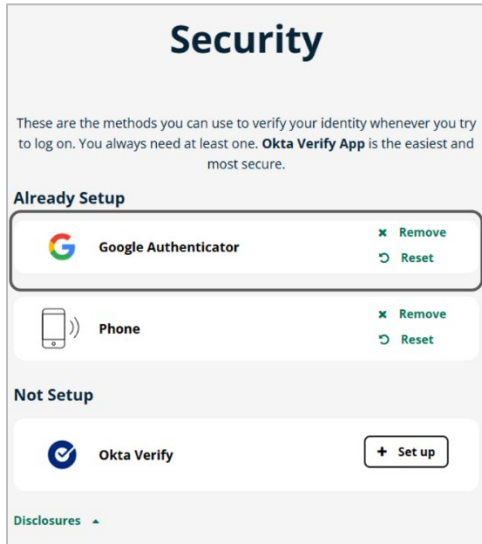


6. Enter code sent to Google Authenticator app in the **Enter code** field and click **Verify**.

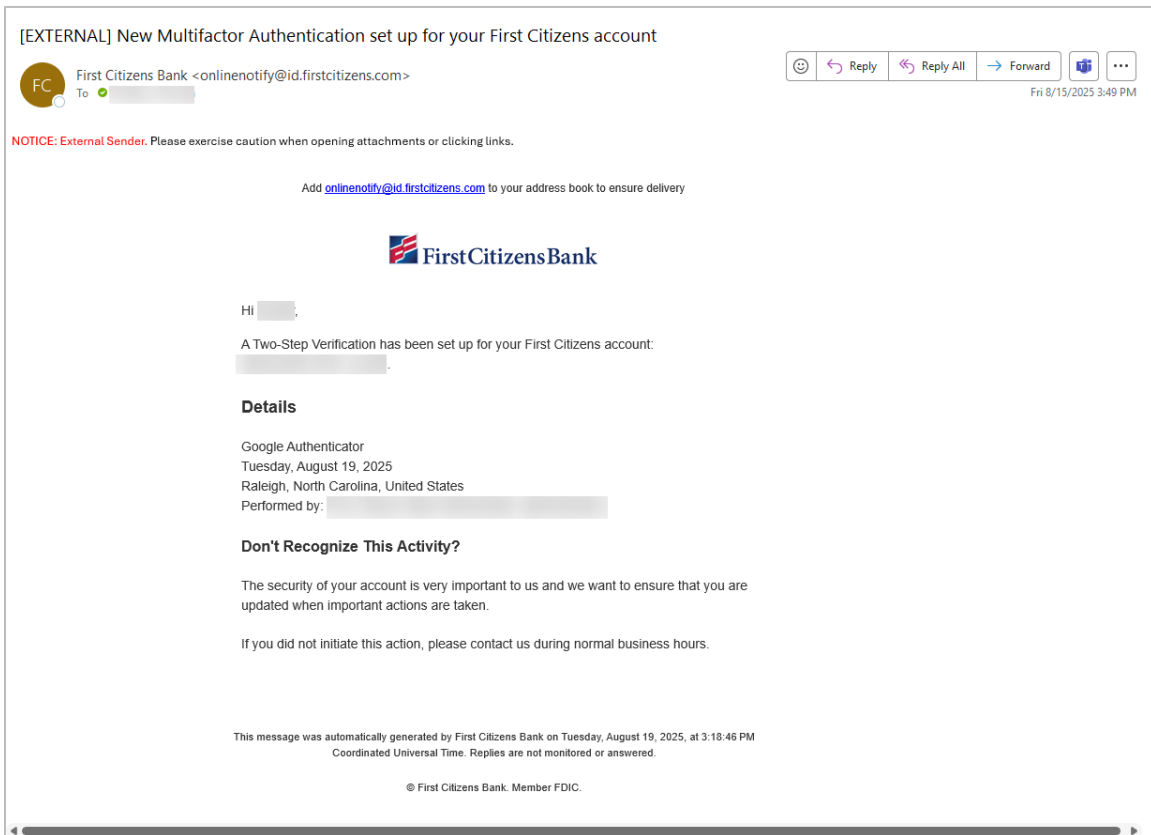


7. **Success 2 step verification complete** success message will display.

8. The **+Set up** button will be replaced with a **Remove** and a **Reset** button.

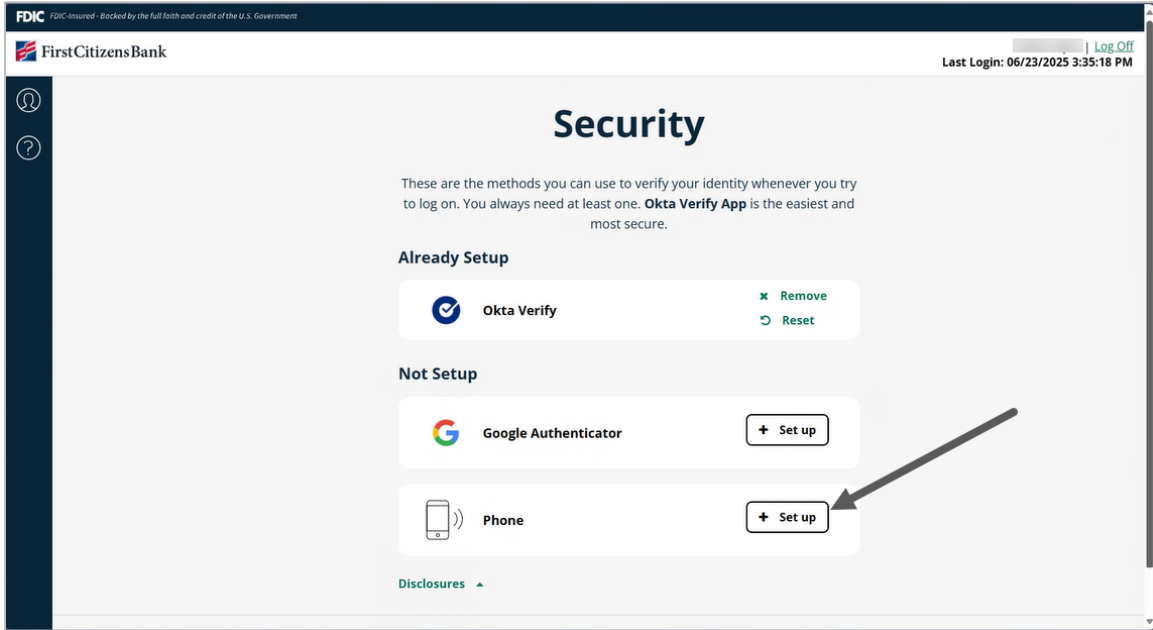


9. The client will receive an email confirming that a multifactor authenticator has been set up.



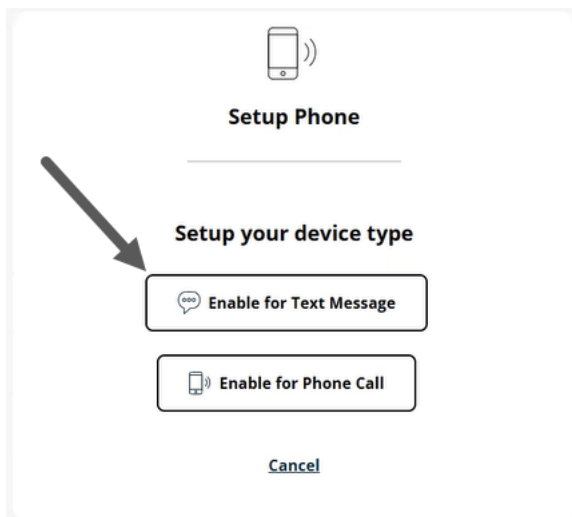
Text Message Authentication (SMS) Enrollment

1. Click **+ Set up** next to **Phone** authentication.

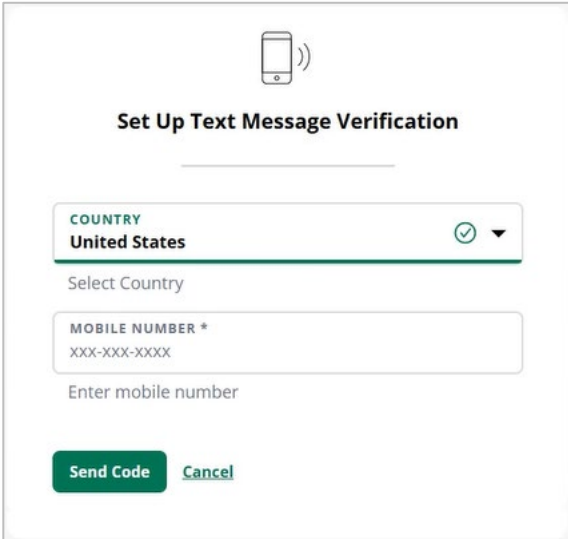


2. Choose the **Enable for Text Message** option.

Note: You can only set up one method for **Phone** authentication. Choose from either **Text Message** **OR** **Phone Call** option. You cannot set up both options.



3. Enter the phone number for your mobile device and click **Send Code**.



Set Up Text Message Verification

COUNTRY
United States

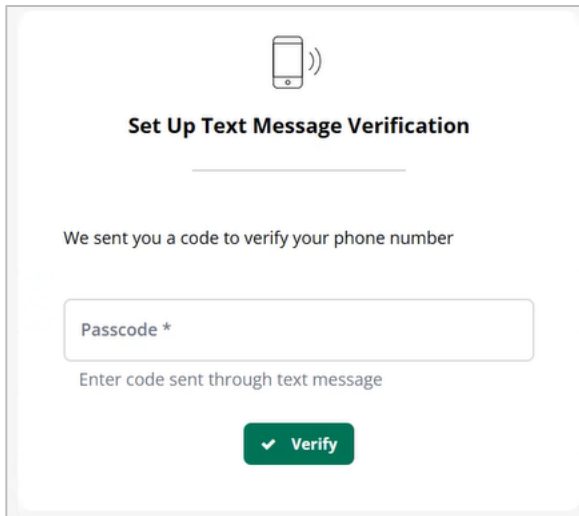
Select Country

MOBILE NUMBER *
XXX-XXX-XXXX

Enter mobile number

Send Code [Cancel](#)

4. Enter code sent to mobile device in **Passcode*** field and click on **Verify**.



Set Up Text Message Verification

We sent you a code to verify your phone number

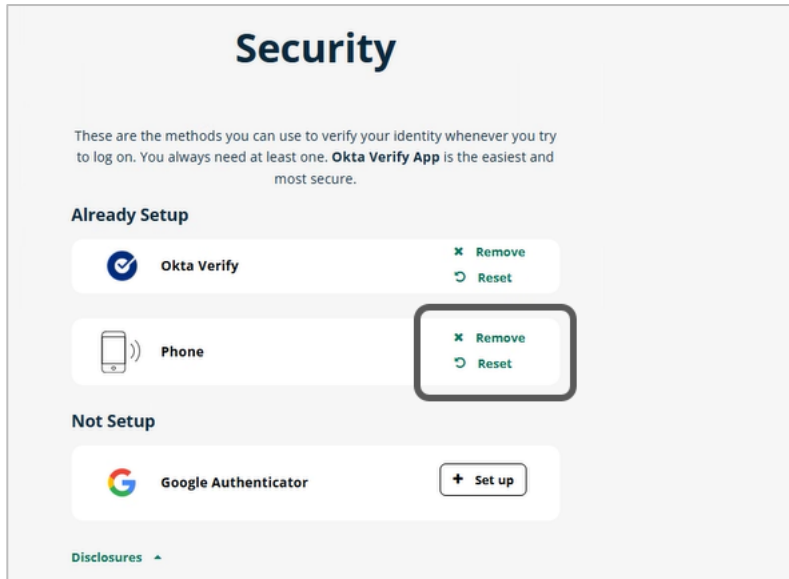
Passcode *

Enter code sent through text message

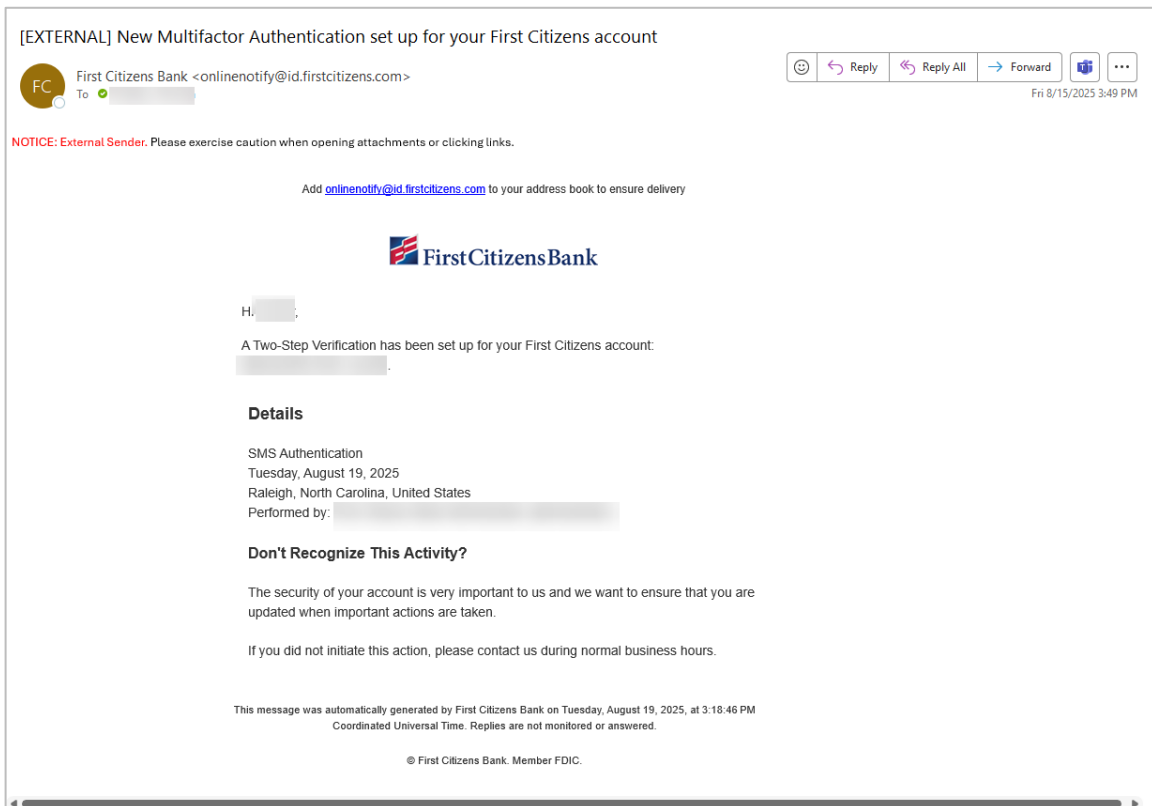
Verify

5. **Success 2 step verification complete** success message will display.

- The **+Set up** button will be replaced with a **Remove** and a **Reset** button.

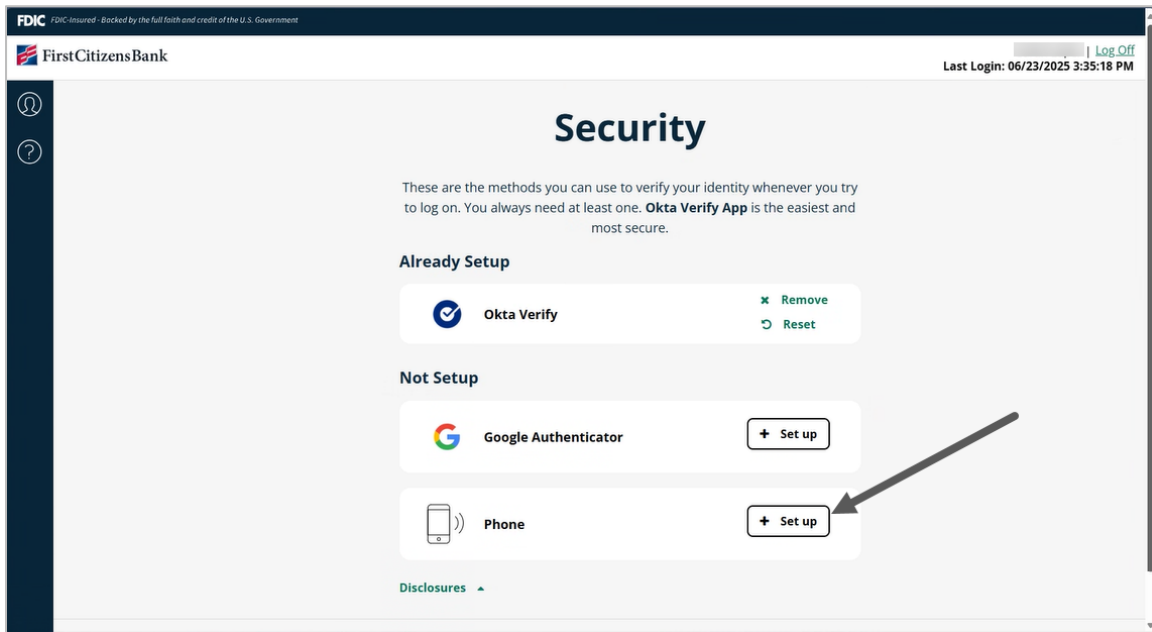


- The client will receive an email confirming that a multifactor authenticator has been set up.



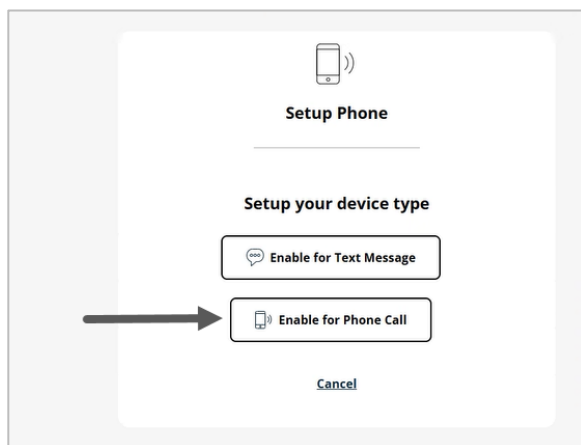
Voice Call Authentication Enrollment

1. Click **+ Set up** next to **Phone** authentication.

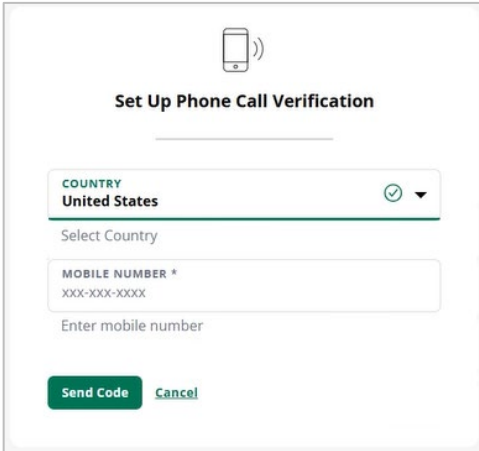


2. Choose the **Enable for Phone Call** option.

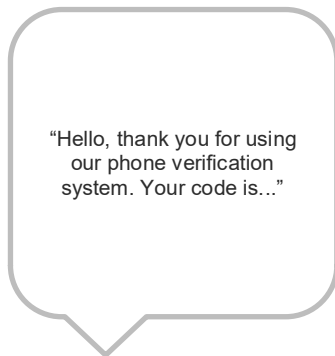
Note: You can only set up one method for **Phone** authentication. Choose from either **Text Message** **OR** **Phone Call** option. You cannot set up both options.



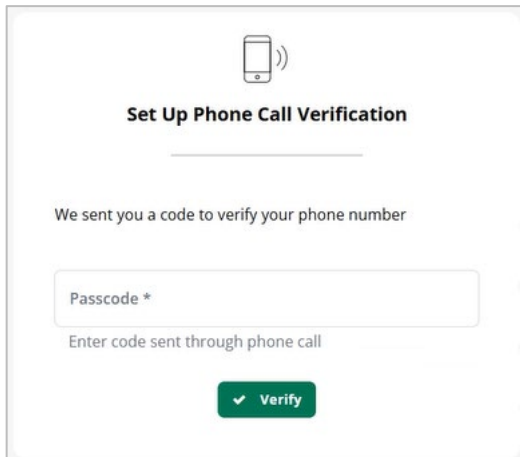
3. Enter the phone number you wish to receive a call on (can be a landline or a mobile device) and click **Send Code**.



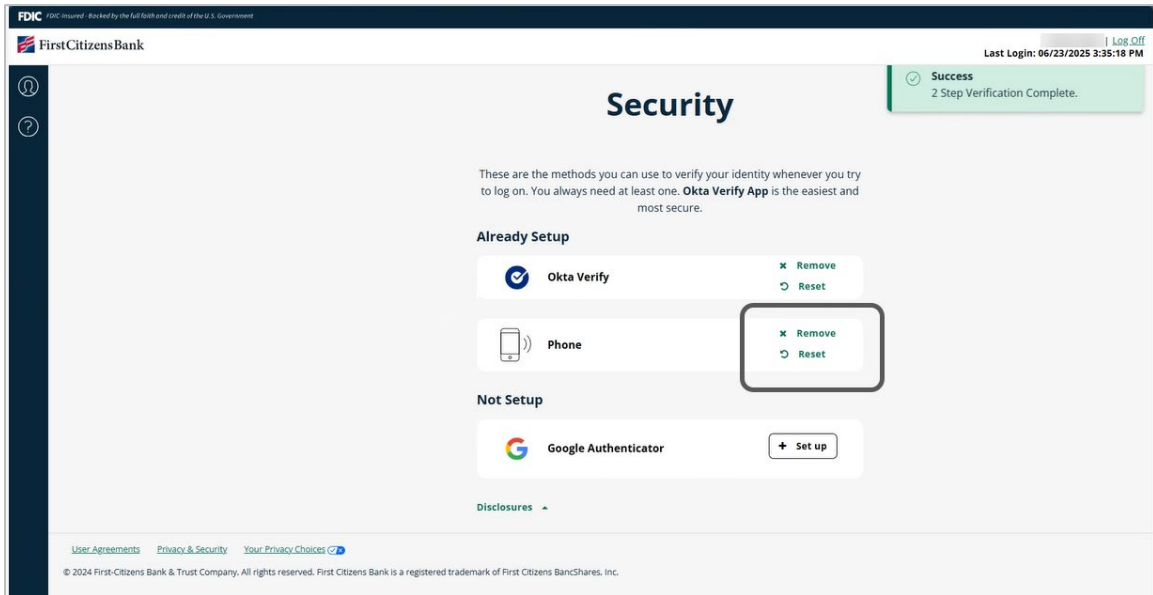
4. Answer the phone call and listen for the code.



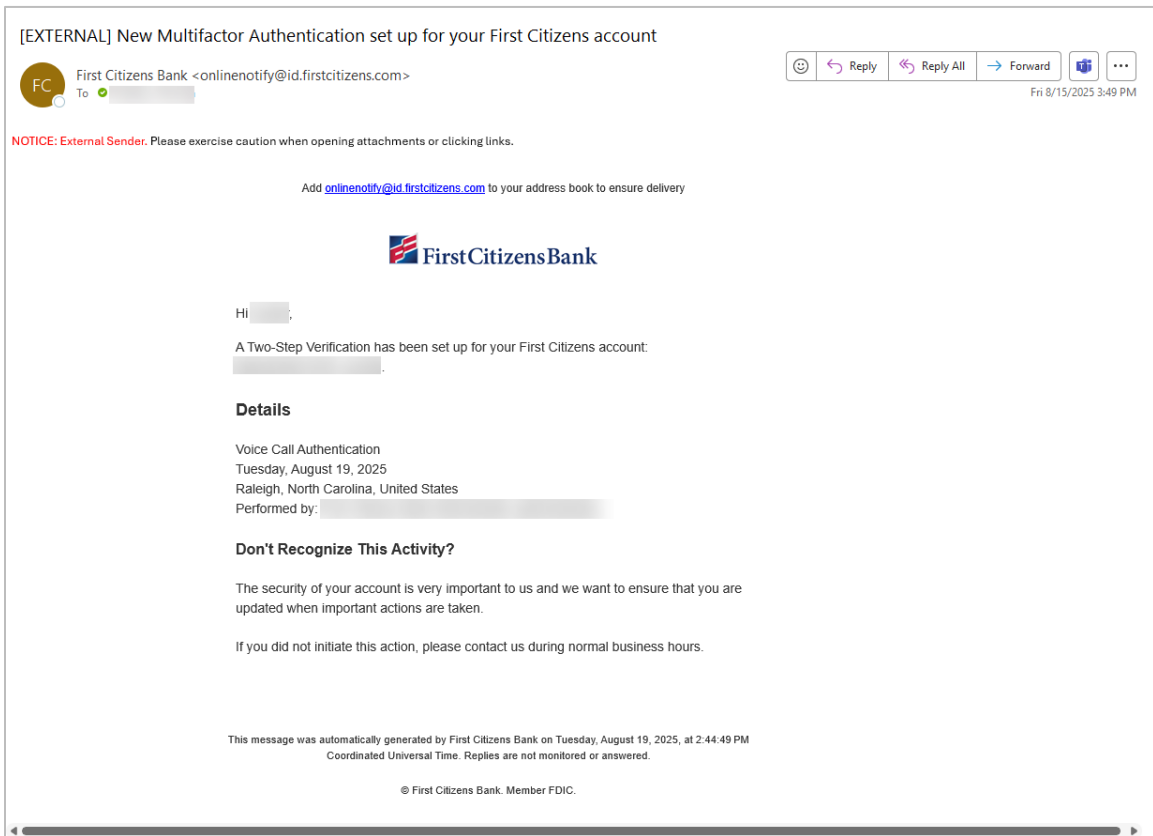
5. Type in the code in the **Enter code** field and click **Verify**.



- The **+Set up** button will be replaced with a **Remove** and a **Reset** button. **Success 2 step verification complete** success message will display.

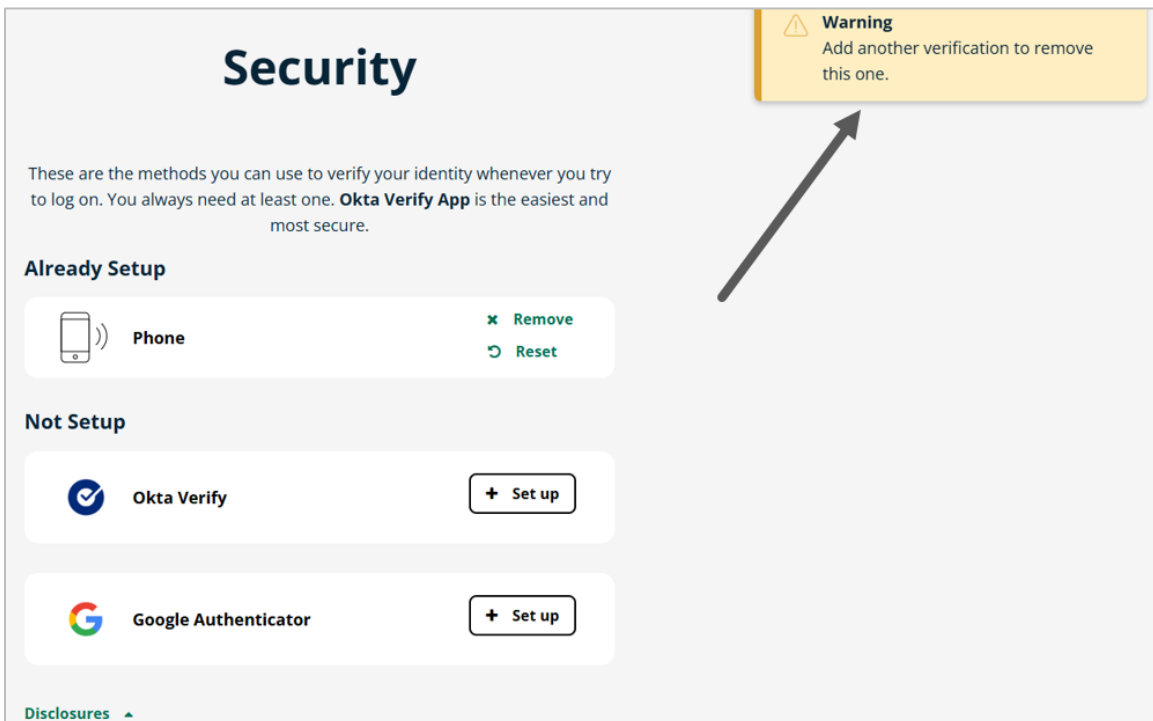


- The client will receive an email confirming that a multifactor authenticator has been set up.



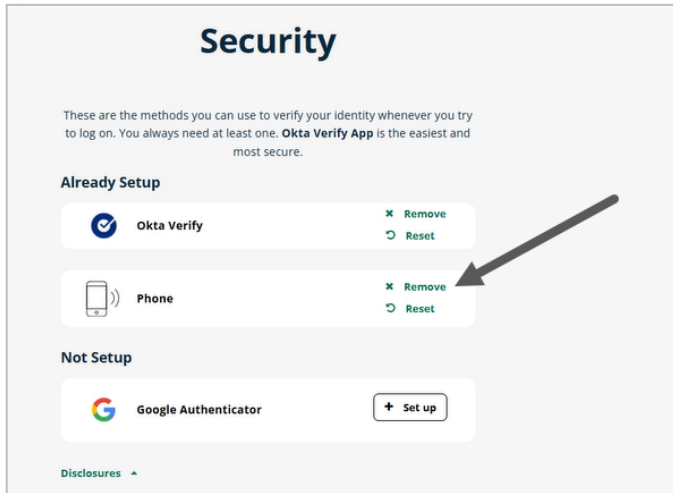
Additional Information for Remove and Reset Options:

1. If you remove a factor, then you will receive an email informing which authentication method is removed.
2. You must always have at least 1 enrolled MFA factor. To **Remove** or **Reset** any factor, there must be 2 or more factors already setup. You cannot **Remove** or **Reset** if there is only 1 factor set up with the account.
3. If you only have one factor enrolled, and you attempt to remove, then you will get an error message.



The screenshot displays the 'Security' settings page. At the top right, a yellow warning box contains a warning icon and the text: 'Warning Add another verification to remove this one.' An arrow points from this warning box to the 'Phone' factor in the 'Already Setup' section. Below the warning, the page is titled 'Security' and includes a sub-header: 'These are the methods you can use to verify your identity whenever you try to log on. You always need at least one. Okta Verify App is the easiest and most secure.' The page is divided into two sections: 'Already Setup' and 'Not Setup'. Under 'Already Setup', there is one factor: 'Phone', which has 'Remove' and 'Reset' options. Under 'Not Setup', there are two factors: 'Okta Verify' and 'Google Authenticator', each with a 'Set up' button. A 'Disclosures' link is visible at the bottom left.

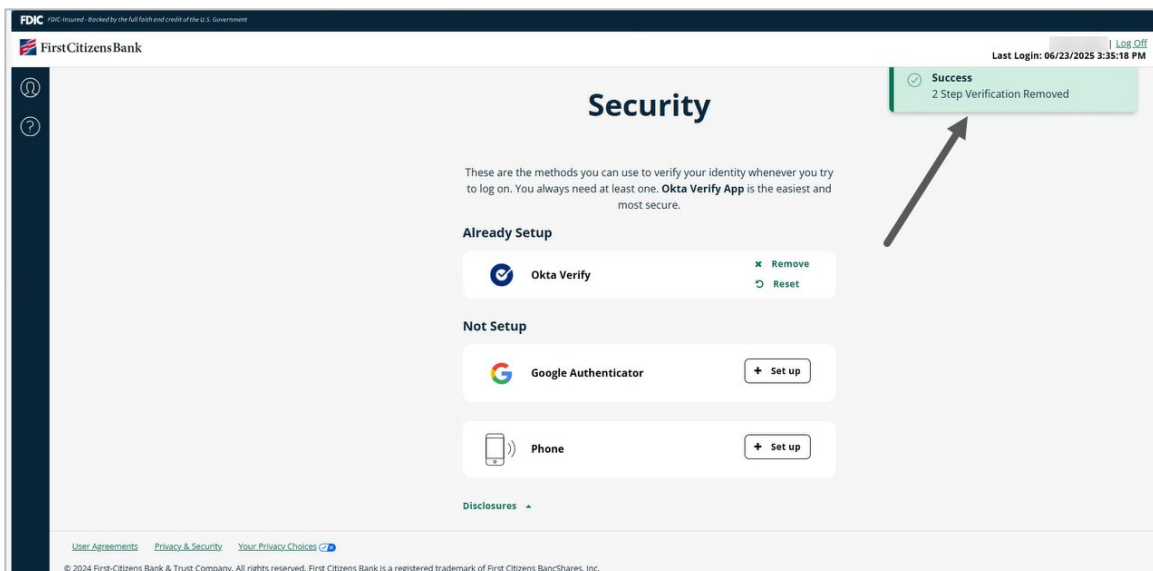
- Once at least two MFA factors have been established, select the **x Remove** option to remove a method.



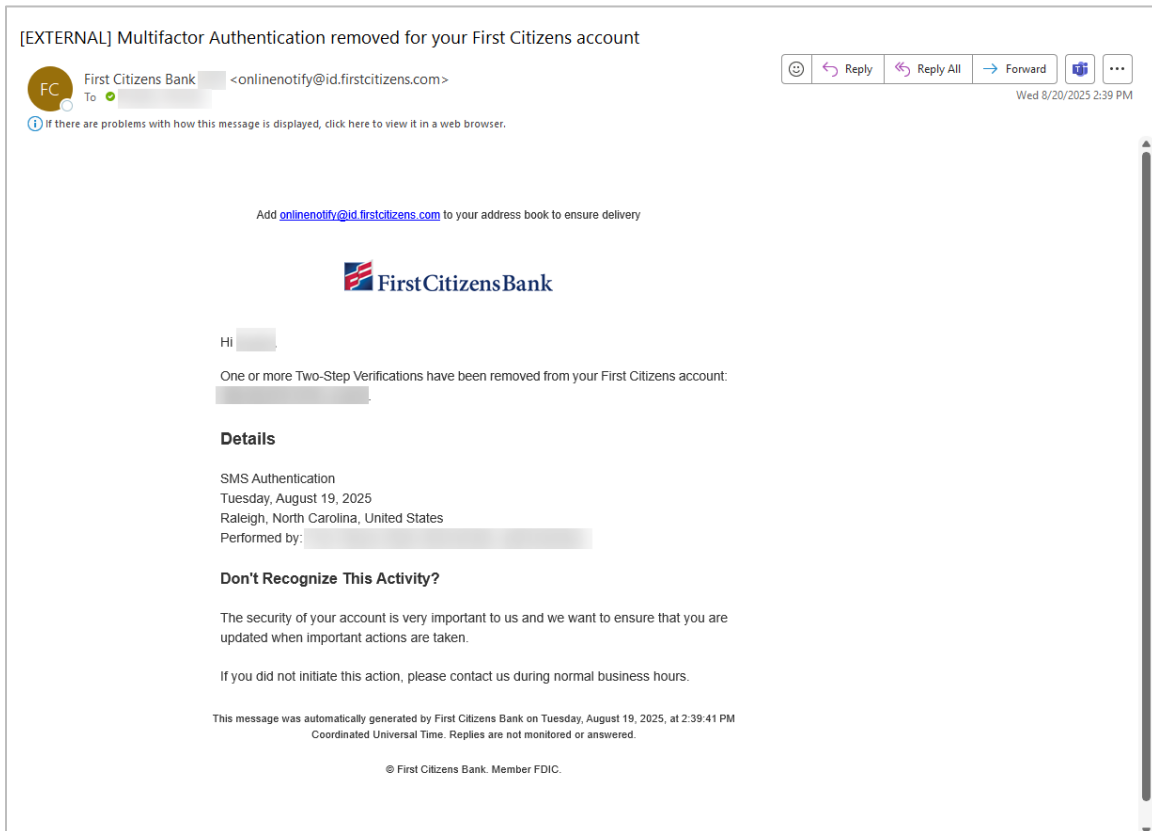
- You'll be prompted with the below pop-up. Select **Confirm** to remove or **Cancel** to keep.



- If you confirm removal of a MFA factor, you'll receive a success message.



7. The client will receive an email confirming that a multifactor authenticator has been removed.




When to use reset and why:

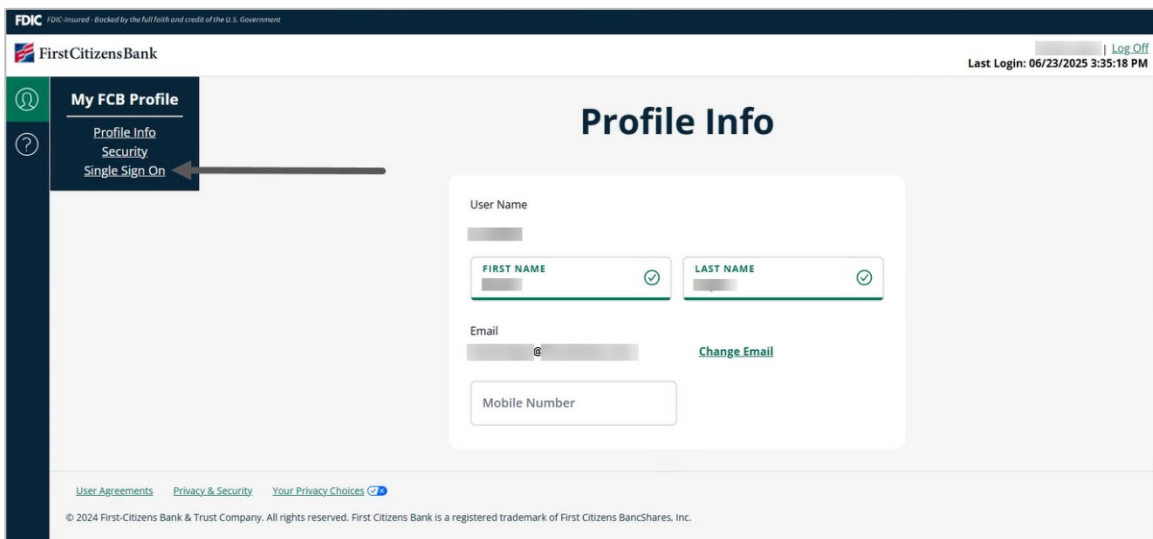
1. For **Reset**, the process is the same as a new enrollment (refer to the new enrollment section of this guide).
2. For Okta Verify and Google Authenticator, the **Reset** button is used if you have a new mobile device. The account on Okta Verify or Google Authenticator on the old mobile device will not transfer to the new mobile device. You will need to re-enroll so that a new account can be added to log in using that factor on the new mobile device.
3. For Phone **Text** and **Call**, the **Reset** button is used if you have a new phone number that needs to be updated, or you want to switch between text and call.
4. If you choose to reset a factor, then you will receive two emails:
 - The first email will confirm removal of the factor.
 - The second email will confirm the setup of the factor.

Single Sign-On

You can merge your existing First Citizens Bank applications, so that you only have one digital identity (Username & Password) to use as a Single Sign-On (SSO) for most of your First Citizens Bank applications.

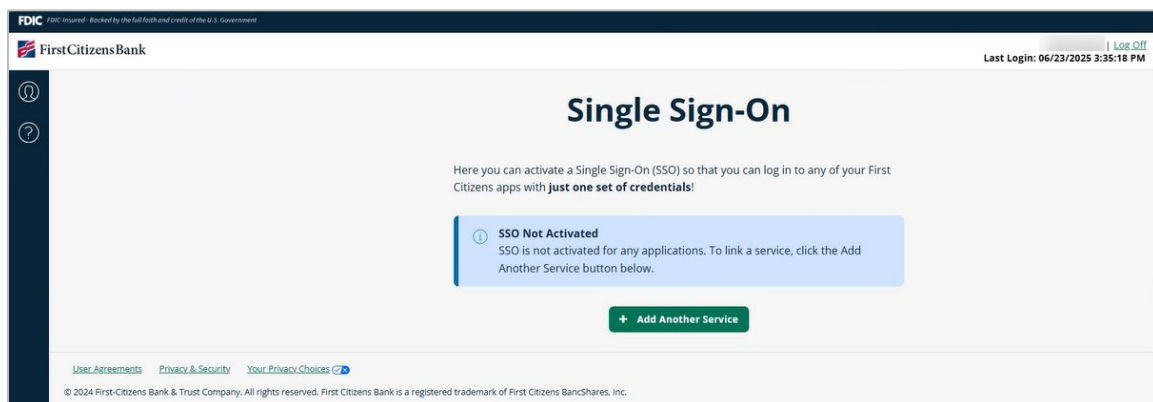
Notes:

- You must be provisioned to more than one First Citizens Bank application to be eligible for SSO.
- Log into the application that you want to establish as the single set of credentials for all your services. The next step is to access Profile Manager from the application that you logged into. Select the **Profile** icon  on the top left corner of the screen, then click on **Single Sign On** as displayed on the screenshot below.



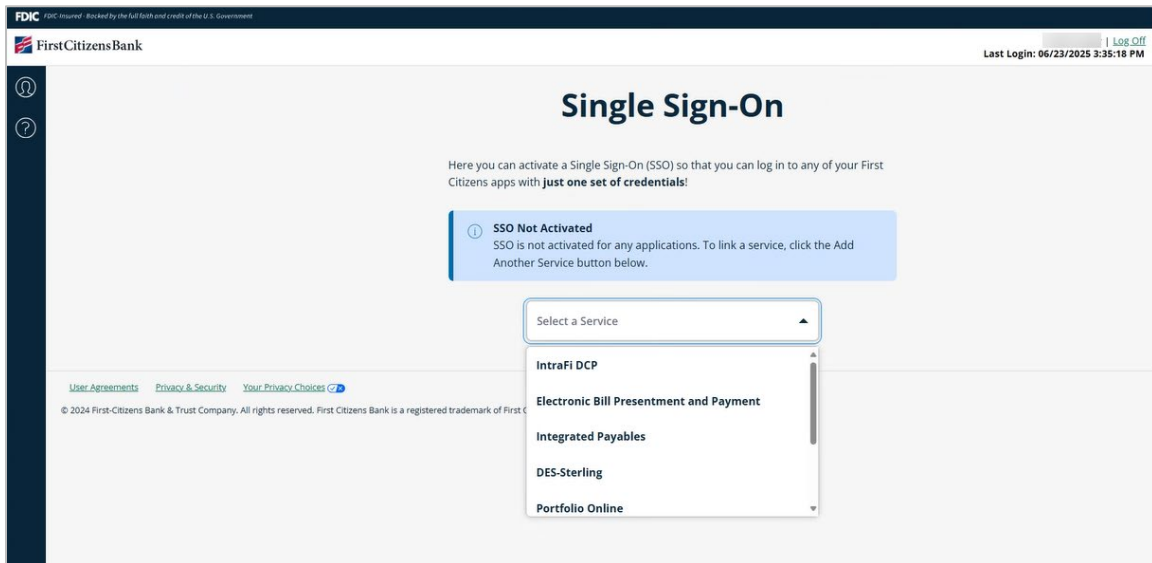
1. Choose the application you wish to merge with by clicking the **+Add another Service**.

Note: You will see the **SSO Not Activated** message as shown below. Once you've completed the merge process, this message will be replaced to display the service(s) you selected to merge. See screenshot in Step 6 for an example.

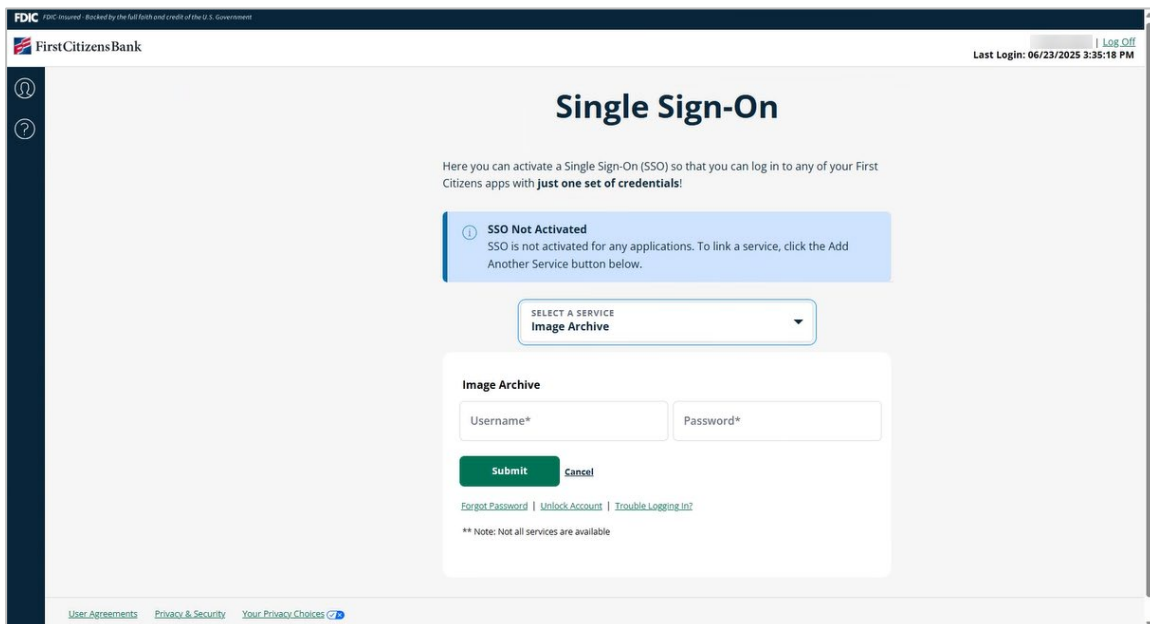


- Choose the application you want to merge from the **Select a Service** drop-down menu.

Note: You will see applications listed in the drop-down for all services that are available to be merged.



- Enter your existing login credentials for the application that was chosen and click **Submit**.



4. Complete the MFA request.

SINGLE SIGN-ON SETUP ×

Verify

Text Message Okta Verify

SINGLE SIGN-ON SETUP ×

Verify

Setup Okta Verify


Click below to verify with the Okta App on your phone:

✓ Send Push or Enter Code

[Try another method](#) | [Trouble Authenticating?](#)

SINGLE SIGN-ON SETUP ×

Verify

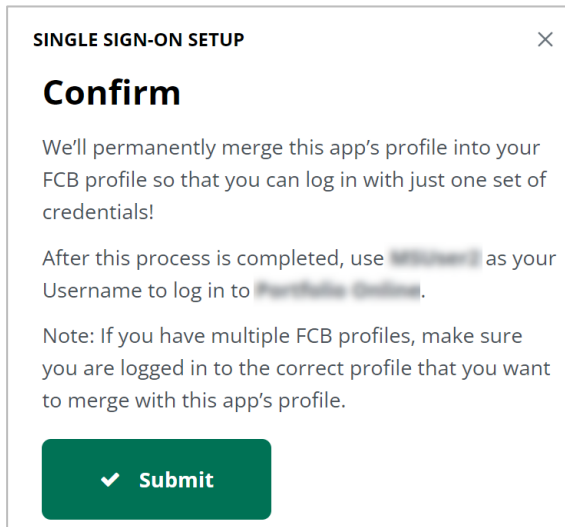
 Google Authenticator


AUTHENTICATION CODE ✓

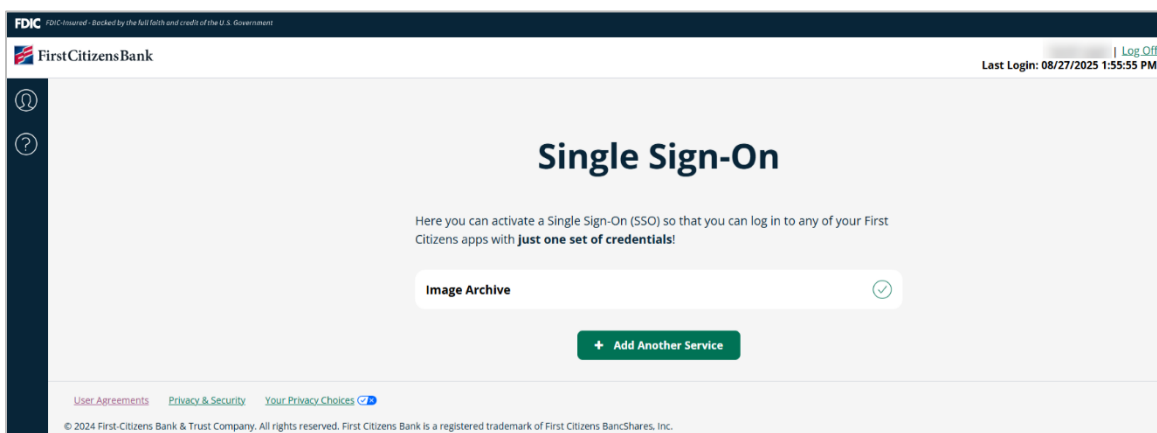
Enter the code displayed in the Google Authenticator app.

✓ Verify

- Once you have gone through all the necessary MFA verification steps, then click **Submit**.



- Once confirmed, the applications selected will be SSO activated. You can now access the merged applications using the single set of credentials you have established which will be listed as you see in the below screenshot with a checkmark icon  next to it.



Disclosures:

Google and Google Docs are trademarks of Google LLC and this user guide is not endorsed by or affiliated with Google in any way.

Okta Content is the exclusive property of Okta and/or its licensor(s). Okta and/or licensor(s) own(s) all right, title and interest in the Okta Content, including but not limited to copyright, trademark, service mark, trade dress, and other applicable worldwide intellectual property rights.