

Dual Authentication Setup

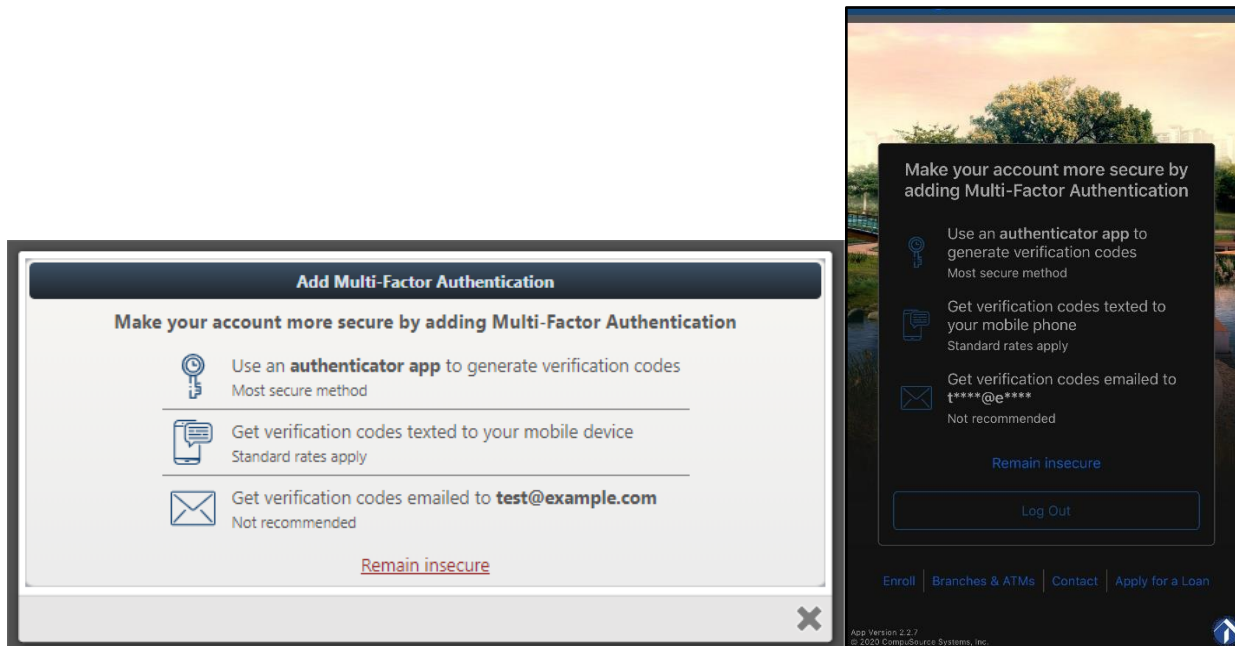
Dual-Factor Authentication (2FA), sometimes referred to as *two-step verification* or *two-factor authentication*, is a security process in which users provide two different authentication factors to verify themselves. This process is done to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication, in which the user provides only one factor -- typically, a password or passcode. Two-factor authentication methods rely on a user providing a password, as well as a second factor, usually either a security token or code that can be delivered via text message or by an authentication software. More advanced authentication can involve biometric factors such as a fingerprint or a facial scan.

Our online banking system is now utilizing Dual Factor Authorization (2FA) as a means to make your remote banking more secure. This security feature should not be taken lightly and though it may introduce added inconvenience to you that is a small price to pay in order to keep your financial information secure.

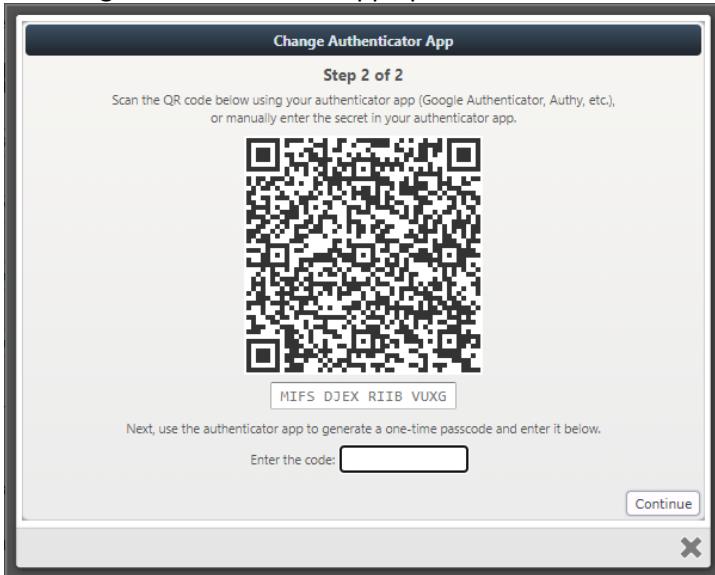
You will have three 2FA methods to choose from as your additional layer of security:

- An 'Authenticator App' is an application that can be added to your mobile device that randomly generates codes what will be available for short periods of time. This code offers a second layer of protection and would be needed to be entered as part of the login process. This is the most secure method available, though it may be daunting for those less tech savvy members.
- Verification codes can be texted to you and that code would need to be entered as part of the login process.
- A verification code can be emailed to you and then entered as part of the login process. This is the least secure method and can be the most cumbersome.

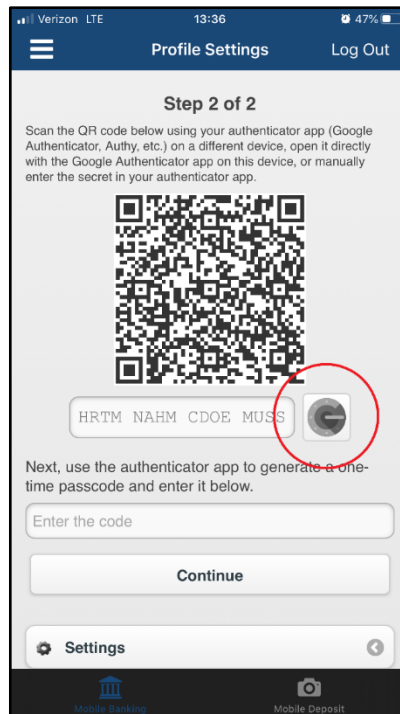
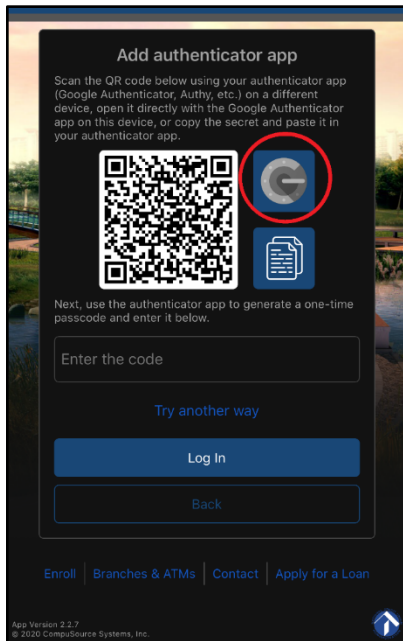
The first screen you will be prompted after login is this (PC/Mobile App):



Choosing the Authenticator App option will lead to the following flow:



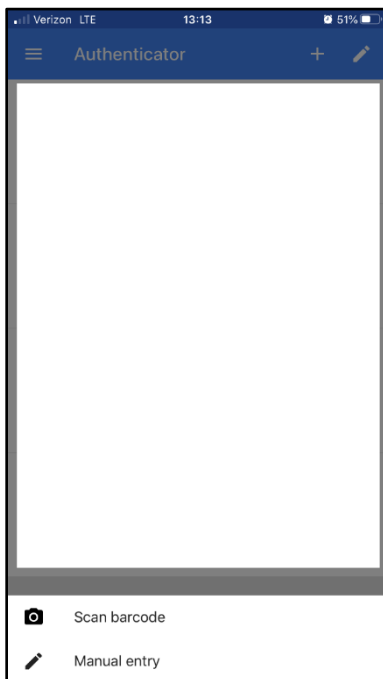
Install a third-party authenticator app. Google Authenticator and Authy are the given examples, but there are other apps that can be used. On mobile, you will also be presented with a button to open Google Authenticator directly.



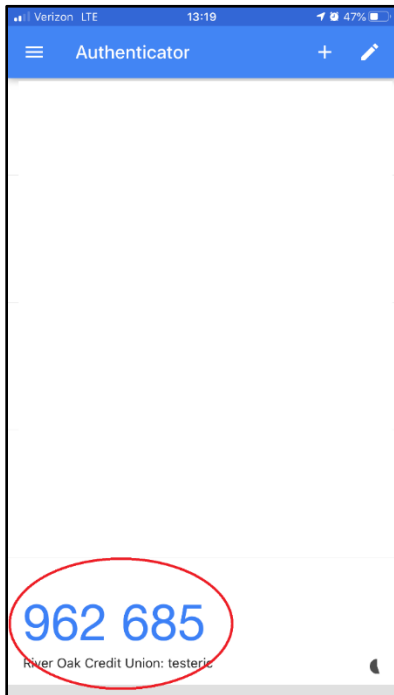
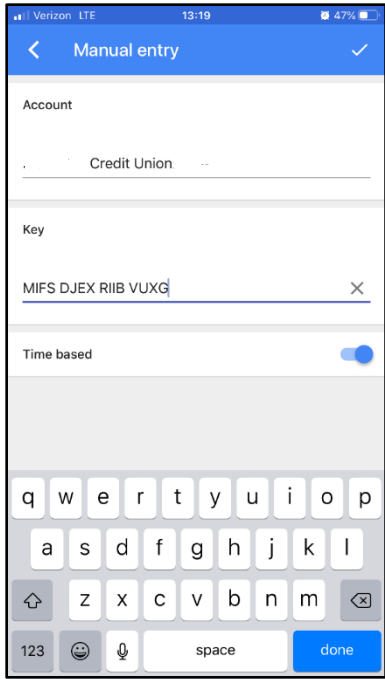
Google Authenticator



Open the app and click on the + on the top right corner of the screen.



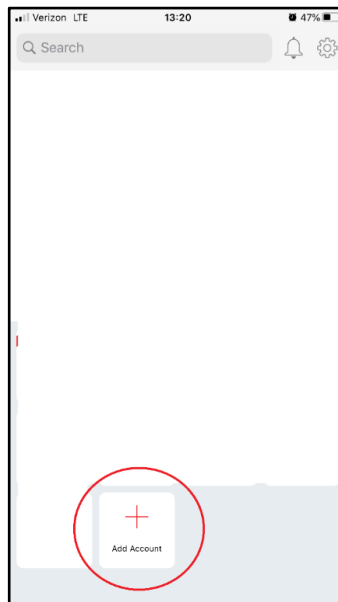
Choose either:
Scan Barcode, which will bring up the camera and allow you to scan the barcode directly. Once scanned, the account is automatically added.
Manual Entry, which will require you to enter the 16-digit secret code into the app (spaces are not required). See next screen.



Now that the account is added, it will generate a new one-time passcode every 30 seconds. This code can be used to complete the setup of the authenticator app.

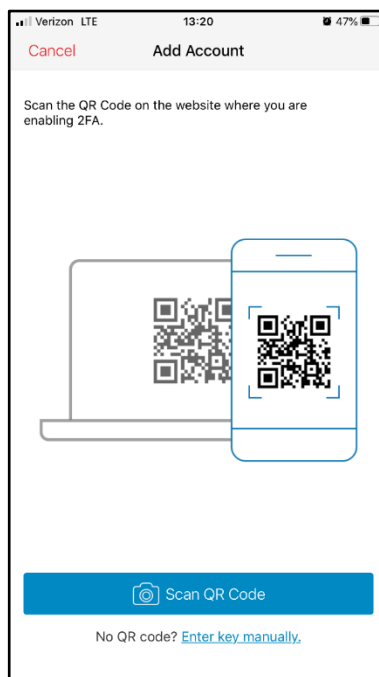
Authy App

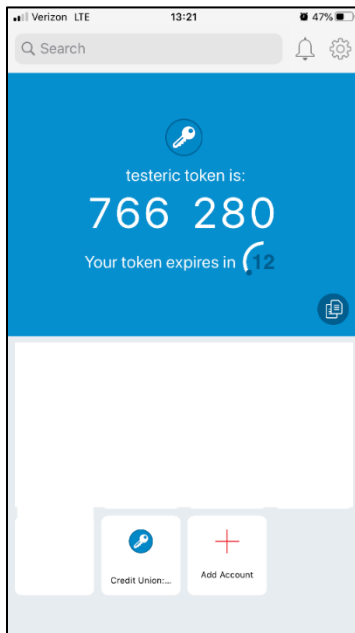
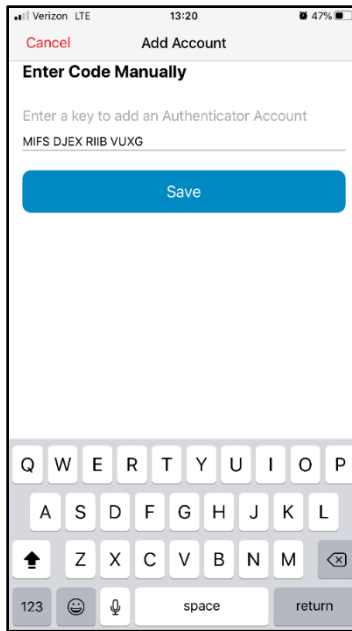
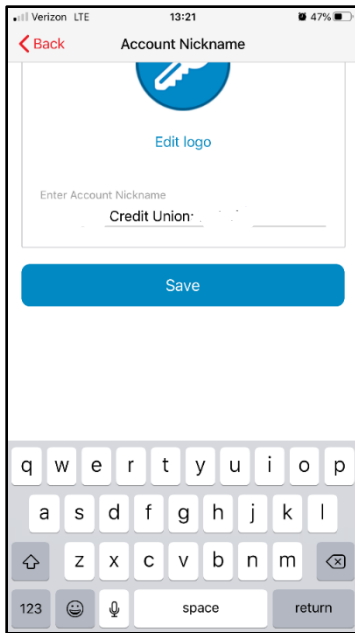
Open the app and click the + on the bottom of the screen.



Choose either:
Scan QR Code, which will bring up the camera. Scanning the QR code will automatically add the account to Authy.

Enter key manually, which will require you to manually enter the 16-digit secret code (spaces not required). See screens below.





Once the account is added, click on the account at the bottom to display the one-time passcode. Passcodes cycle every 30 seconds.

Anytime you are prompted for a one-time passcode, you simply open your app and find the credit union online banking account, and use the code displayed.

Get Verification Codes Texted to your Mobile Device (PC and Mobile screens below)



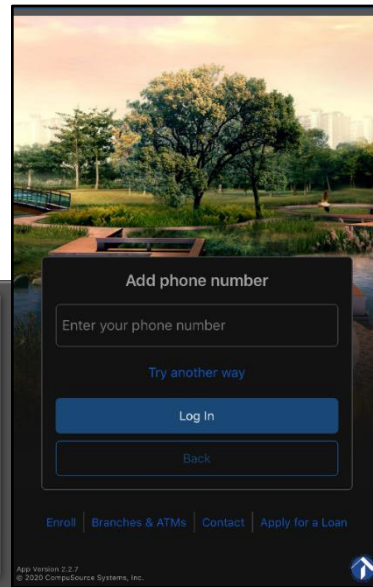
Add Multi-Factor Authentication

Step 1 of 2

Enter your new Phone Number below:

Phone Number:

[Back](#) [Continue](#)



Add phone number

Enter your phone number

[Try another way](#)

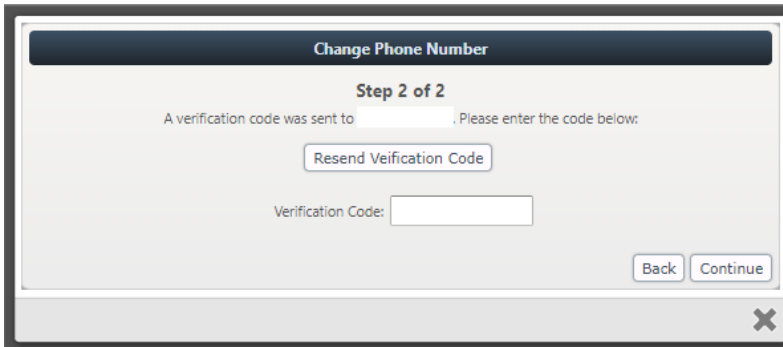
[Log In](#)

[Back](#)

[Enroll](#) | [Branches & ATMs](#) | [Contact](#) | [Apply for a Loan](#)

App Version 2.2.7
© 2020 CompuSource Systems, Inc.

Once setup, you will be prompted to enter the code that was sent to your mobile device.



Change Phone Number

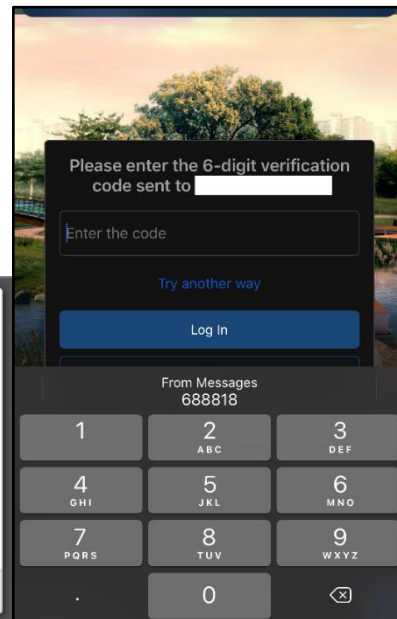
Step 2 of 2

A verification code was sent to . Please enter the code below:

[Resend Verification Code](#)

Verification Code:

[Back](#) [Continue](#)



Please enter the 6-digit verification code sent to

Enter the code

[Try another way](#)

[Log In](#)

From Messages
688818

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
.	0	<input type="text"/>

The process flow is the same for the email dual factor authorization method; excluding the prompt to enter your email address, as it's a required field during initial enrollment.