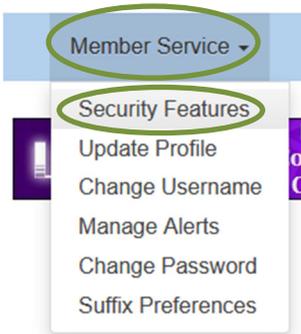


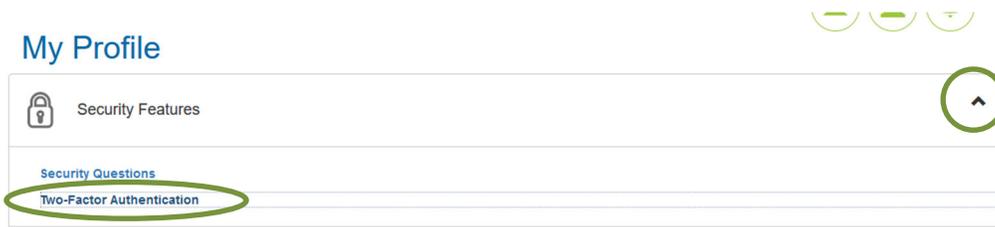
## Online Banking: Multi-Factor Authentication or MFA

Multi-Factor Authentication (MFA) is a security enhancement in which a user is granted access only after successfully presenting two or more pieces of evidence: something you know (password) AND something you possess (cellphone/telephone). If you turn on MFA, any event that would normally present your “Security Questions” will instead ask you for a code texted to your cellphone. MFA is an extra layer of security that makes it harder for thieves to log in as if they were you. The step by step instructions below has been created to assist you learning about this new enhancement.

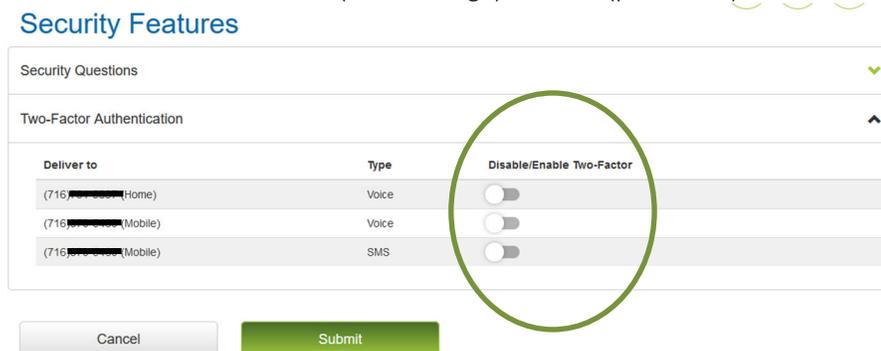
- By default, current Online Banking Members will **be opted out** of MFA.
- After Tuesday, July 28<sup>th</sup> any Member that signs up for Online Banking will be prompted to use MFA or opt out of MFA.
- A Member can opt in by logging into Online Banking, navigate to the “Member Service” tab and then click “Security Features.”



- Then, under My Profile, expand the “Security Features” box and select “Two-Factor Authentication” as shown below:



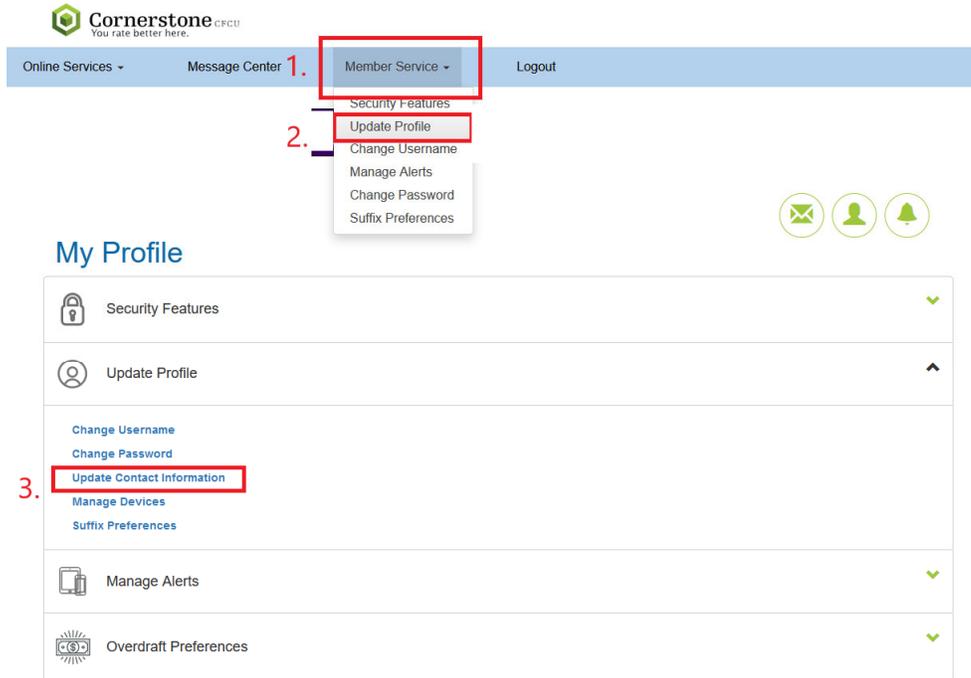
- On this page Members can enable MFA and choose which number the message should be sent to. Members can also choose between SMS (text message) or Voice (phone call) as shown below:



NS3 Release 2.19.3 | 44DE77 | R | © 2020 - Share One, Inc.



If a Member would like to add a new phone number for MFA, follow the 3 steps below to get to the update contact info page:



The screenshot shows the Cornerstone Member Service navigation bar. Step 1 highlights the 'Member Service' dropdown menu. Step 2 highlights the 'Update Profile' option within the dropdown. Step 3 highlights the 'Update Contact Information' option within the 'Update Profile' sub-menu. Below the navigation bar, the 'My Profile' section is visible, with 'Update Contact Information' also highlighted in red.

NS3 Release 2.19.3 | 44DE77 | R | © 2020 - Share One, Inc.

After Tuesday, July 28<sup>th</sup>, any Member that signs up for Online will be prompted to use MFA. Members can opt of it, but they will be notified about it until they either enable MFA or opt out of it. The notification below will appear until the Member requests to no longer receive this warning.

You have not opted to use any phones for two factor authentication.  
Not interested? Click [here](#) to no longer receive this warning.

When a Member does enroll in MFA, it will replace their security questions. MFA will not happen on every login, only when unusual behavior happens. Instead, anytime a Member would normally be prompted to answer a security question, they will instead have to pass an MFA prompt. The following is what the prompt will look like when logging in.

- The Member will first have to choose what method and what number.

## Security Challenge

You are required to complete a security challenge to access your account and have opted in for both SMS and Voice challenges. Please choose a method and number from the options below. We will call or text you at this number and give you additional instructions. If you do not recognize these numbers, do not proceed; call the Credit Union for assistance.

**Challenge Method**

SMS

SMS

Call

Cancel

**Phone Number**

▼

Next



- Then the Member will either get a SMS message (text message) like the one shown below:

**Text (SMS)**

For this first example let's look at text (SMS) authentication. The member receives a message on their phone reading "Message from [Your CU]..." with a confirmation code.



The Challenge screen now displays a **Confirmation Code** field in which they place the code.

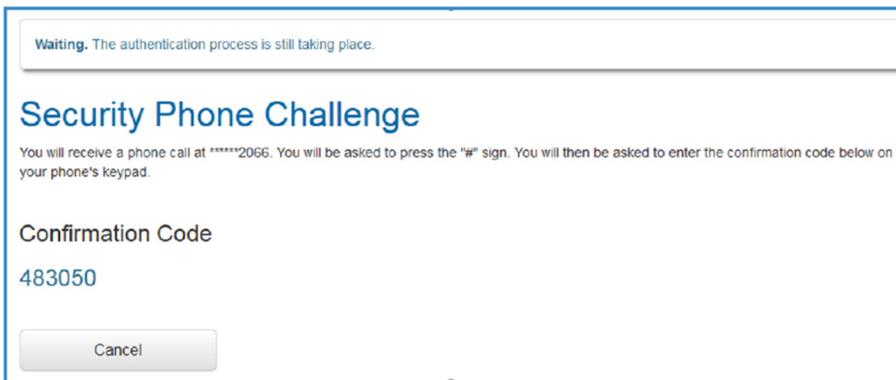


The screenshot shows a "Security SMS Phone Challenge" screen. It includes instructions: "You will receive an SMS Text Message at \*\*\*\*\*2066. The SMS Text Message will contain a confirmation code. When you receive the SMS Text Message, enter the confirmation code in the box below and press 'Submit'." Below the instructions is a "Confirmation Code" label and a text input field containing "ZD2GUY". At the bottom are "Cancel" and "Submit" buttons.

- Or the Member will receive a phone call:

**Voice**

Next let's look at a voice challenge. Instead of receiving a text, the member receives a confirmation code on the screen itself along with instructions on how to authenticate once they receive the call:



The screenshot shows a "Security Phone Challenge" screen. At the top, it says "Waiting. The authentication process is still taking place." Below that are instructions: "You will receive a phone call at \*\*\*\*\*2066. You will be asked to press the '#' sign. You will then be asked to enter the confirmation code below on your phone's keypad." Below the instructions is a "Confirmation Code" label and the code "483050" is displayed. At the bottom is a "Cancel" button.

They'll press "#", enter the code, then be taken to their Account Summary once it is authenticated. If members click **Cancel** for voice or text authentication they are taken back to the login screen.

