TWO-FACTOR AUTHENTICATION (2FA)

What is 2FA?

2FA, or Two-Factor Authentication, sometimes referred to as two-step verification, serves as an extra layer of security for stronger protection of your online accounts.

When enabled within online banking, you will need to enter your password (first factor) and then provide a second security code (second factor) from one of the following: text message, email, voice message or 2FA app. You, and anyone else, won't be able to access your credit union accounts until both factors have been successfully provided.

Enable 2FA within Online Banking:

- 1. Login to Online banking via web browser.
- 2. Go to the top right drop down menu and select "Settings" then click on "Security."



3. Toggle "Require Two-Factor Authentication For Each Login" to the **ON** position and enable the options you'd like to use.

Two-Factor Authentication		Require Two-Factor Authentication For Each Login $$ $^{\odot}$	OFF	O ON	When enabled, mandatory two-factor	
	EMAIL CODE	1 email address on file	ENABLED	1	authentication will require the user to always validate their identity through one of the two- factor authentication methods setup below, regardless of any other security settings such as "Remember this Device."	
	CODE VIA SMS	2 SMS-enabled phone numbers on file	ENABLED	/		
	CODE VIA VOICE CALL	2 phone numbers on file	ENABLED			
	2FA APP	Authentication app not enabled	DISABLED	1		

4. Next time you login you will see this prompt.

Verification needed		Enter code
e «	(***)******	A 6-digit code has been sent to your phone number ending in
SMS Email Call	()	Enter Code The Code Will Expire In 15 Minutes
	Mandatory Two Factor Authentication has been enabled.	Resend code
	Back Send code	Back Verify

You have now enhanced your online banking security with two-factor authentication (2FA)

