Mobile App Authentication Frequently Asked Questions

Toll free & text: 800-333-9571 Web: https://www.questfcu.com

What is MACO?
MACO stands for Mobile Authentication Convenience Options.

Is there a certain phone needed to support this feature?
MACO is compatible with both Android and Apple devices. If your device is compatible with mobile banking, you will be able to use the biometric logins. However, if your device does not support a biometric option, it may not be available.

Which MACO option is the most secure?
No single authentication option should be looked at as being more secure than the others. Ultimately it comes down to a member's own usage and their environment. For example, if a member configures a '1234' pin to unlock their phone and then uses the same weak password to authenticate into mobile banking, they are using these security options in the least secure way possible. The same could be said for all other authentication options. Quest Federal Credit Union does not recommend one method over any available methods, but encourages our membership to use strong passwords, not to reuse simple passwords that are easily guessed, and to change passwords and PINs regularly.

I have multiple accounts at the credit union. How do I get MACO to work with all my accounts?
At this time, MACO is only supported for use to log on to one of your accounts per device.

Are MACO options more secure than ID/password/challenge questions?
Biometrics will still have the same vulnerabilities that passwords do today. It is not about enhanced security, it is about convenience. If you share your password and security question with someone today, write them down, or otherwise have your credentials compromised (for example with keylogging malware), then others can access your account. Similarly, if you allow someone to take an up-close video of you blinking and give them authenticated access to your device, then they can access your account.

If I share my phone/device with other people, should I use MACO?
MACO pairs your registered biometric information to the physical device (phone, tablet, etc.). Therefore, it is not recommended to use shared devices with MACO.

I was able to spoof/beat the face by holding it up to a video of me. This seems like a security issue.
Biometrics have the same vulnerabilities that passwords do today. It is not about enhanced security, it is about convenience. If you share your password and security question with someone today, write them down, or otherwise have your credentials compromised (for example, with keylogging malware), then others can access your account. Similarly, if you allow someone to take an up-close video of you blinking and allow them authenticated access to your device, then they can access your account.

Mobile App Authentication Frequently Asked Questions

Toll free & text: 800-333-9571 Web: https://www.questfcu.com

I want to unenroll in one of the MACO options, how do I do that?
In the Settings & Info section of the Mobile App, you can unenroll from each MACO by changing the switch to the "off" position. The Settings & Info section also allows you to remove your MACO profile from the device, which unenrolls you from all MACO. (Use "Reset App Data.")

My mobile device was lost or stolen. What should I do?
In the Settings & Info section of the Mobile App, you can remove your MACO profile on all devices. (Use "Reset Authentication Options on All Devices.") If you have a profile on another device, use this method to disable the profile.

If you do not have a profile on another device, enroll in MACO on a new device and then disable the profile using the directions above. Copy instructions are provided the first time you enroll in a MACO on the new device.

If no device is available, credit unions can contact a CSR to start an Answer Book incident and request that the member's profile be archived. This will disable the profile.

Can I select my own phrase when enrolling/using the voice authentication?
No, personalized phrases are not supported.

Will I have to log in the same way every time or can I switch between the different logins?
You are not required to log in the same way every time. You can use a different MACO, or you can use the standard login of username, password, and security question answer. The Mobile App will default to the last MACO used the next time you log in.

Can I lock myself out of the face recognition, PIN, voice recognition or fingerprint login process?
After several failed MACO authentication attempts, you will be temporarily locked out of authenticating with any MACO, regardless of which MACO authentication caused the lockout. Click "Temporarily Locked," to read a message stating that you have exceeded the allowed attempts and are temporarily locked. You can still log in using the standard login of username and password.

This type of lockout occurs the first three times you are locked out. The lockout time increases with each lockout. You will be unable to use MACO for fifteen minutes, then twenty and then twenty-five minutes. After the lockout period, MACO will unlock, and you can use them as before.

At the fourth lockout, your MACO profile will be disabled. This means you cannot authenticate using MACO on any device. You will see a message saying that "Re-enrollment is required." To use MACO again, click "Settings" to go to the "Settings & Info" section of the Mobile App. Use "Reset Authentication Options on All Devices" to reset your profile. Then (still in Settings & Info), turn the switch for a MACO to the "on" position. This will allow you to re-enroll in the MACO. You will be presented the MACO User Agreement during this authentication.