MACO (Multi-Authentication Convenience Options)

Fingerprint, Face Recognition, PIN,
and Voice Recognition

Introduction

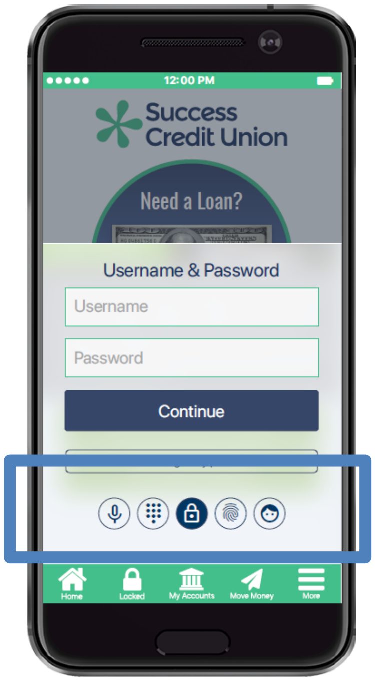
This booklet covers MACO, a convenience option designed to give your member more options for authentication in Mobile App. MACO includes four convenience options: fingerprint, face recognition, voice recognition, and PIN. Included in this booklet is an overview MACO, how to get started, and more. It also shows step by step what the member sees on their device as they enroll and authenticate using MACO.

Contents

Revision date: December 21, 2023

MACO Overview

This section of the booklet provides a brief overview of access, enrollment and, authentication using the four Membership Authentication Convenience Options (MACO). For more pictures and steps of what the member sees, refer to page 9.



Access

To authenticate using MACO, the member taps the appropriate button at the bottom of the login pane (or swipes to the login pane of the desired MACO method during the introduction promotion). *(See image to the left.)*

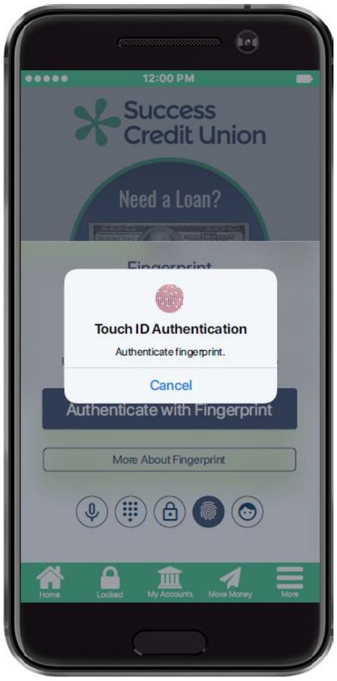
First Step is Standard Authentication

When the member selects to enroll in a MACO method, they must first authenticate by entering their standard login credentials (username, password, and security question answer). After enrollment, the standard authentication is not required; however, it can always be selected in place of MACO.

MACO Use Agreement (Presented One Time)

The member is presented your credit union's MACO User Agreement after the standard authentication. This is presented only one time during the first MACO enrollment. The member is not presented the Use Agreement with other MACO enrollments.

The member is presented the Use Agreement again in these situations: when the Agreement is updated, when the member uses a different device, or if the member unenrolls from all MACOs and then re-enrolls.

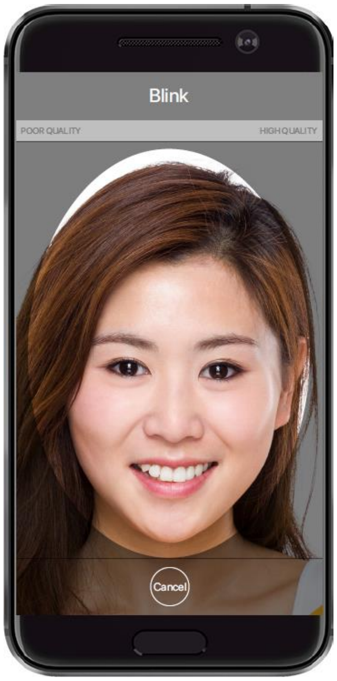


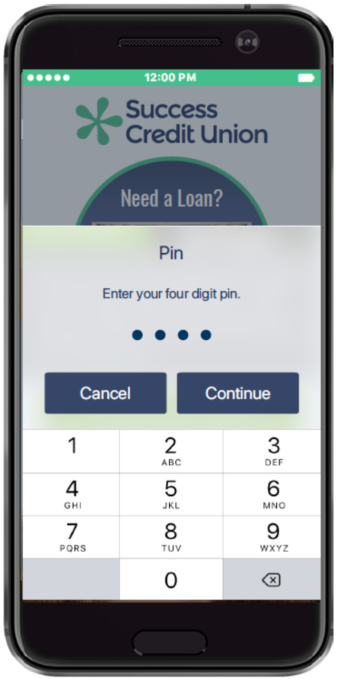
Fingerprint

NOTE: Fingerprint authentication will only show on devices that support it. To use fingerprint authentication, the member must first save a fingerprint sample in the operating system of the device.

During MACO fingerprint enrollment, the member touches the sensor of their device (for example the Home button) to verify they have a match with the fingerprint saved in the operating system of the device.

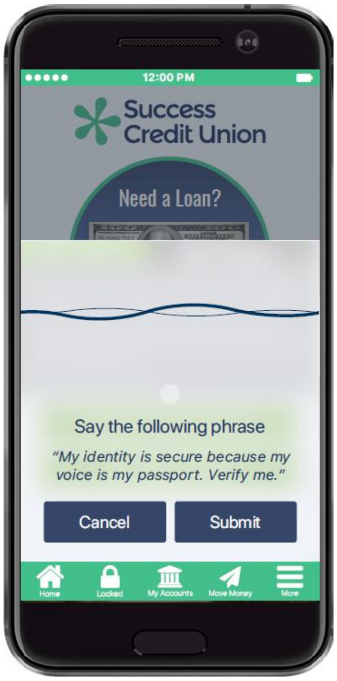
During MACO fingerprint authentication, the member places their finger on the device's sensor. If the fingerprint matches the fingerprint saved in the device's operating system, the member is logged on to Mobile App Banking.





Pin

Enter your four digit pin.



Say the following phrase

"My identity is secure because my voice is my passport. Verify me."

Face Recognition

During face recognition enrollment the device camera takes several pictures of the member. Helpful messaging assists the member to align their face in the proper manner. The best photo is analyzed according to a series of measurements which may include eye socket depth, distance between the eyes, the width of the nose. An encrypted metric assigned to the photo is sent to the DAON server. (The actual photo is not sent to DAON.)

During face recognition authentication, the member gives a live-test sample by blinking (shaking or nodding) which causes the camera of the device to take a photo of the member. The photo metrics are sent to the DAON server. If the photo metric matches what is saved on the DAON server, the member is logged on to Mobile App Banking.

If the member is using a device with Apple Face ID, MACO will adjust to use this authentication method.

PIN

During enrollment the member is presented a number pad on the screen of their device. They tap a four-digit PIN and then tap it again to confirm the number. An encrypted PIN is sent to the DAON server.

During PIN authentication, the member taps their PIN twice in the number pad that is presented. If this PIN matches the number saved on the DAON server, the member is logged on to Mobile App Banking.

Voice Recognition

During enrollment the member says a passphrase that is presented on the screen. Three acceptable recordings are captured, and the best is converted to encrypted voice data that is sent to the DAON server.

During voice recognition authentication, the member is asked to say the phase again. The voiceprint is compared with the audio data on the DAON server. If a match is found, the member is logged on to Mobile App Banking.

LEARNING MORE ABOUT MACO

Getting Started with MACO Brochure (MACO Info Sheet)

Interested in getting started with MACO? Look no further that the Getting Started brochure provided by the Internet Retailer Support Center (IRSC) in the IRSC store. (See below.) This brochure covers highlights of implementing MACO at your credit union, pricing, and frequently-asked questions.

https://irsc.cuanswers.com/wp-content/uploads/2018/01/maco_info_sheet.pdf

IRSC Online Store

Start the implementation of MACO at your credit union by purchasing MACO in the IRSC store. On the store page you will find more information on pricing and the "Getting Started" brochure. You will select whether to prepay for your license or to "true-up" at the end of the calendar year.

https://irsc.cuanswers.com/product/maco-multiple-authentication-convenience-options/

Watch the "Getting Started with MACO" Video Conference

Want to get a big picture of starting MACO at your credit union? Watch a previously recorded session where the Internet Retailer Support Center (IRSC) introduces MACO and performs a live demo of the product.

https://ondemand.cuanswers.com/launching-maco-with-cuanswers-mobile-apps/

Internet Retailer Support Center Website

The Internet Retailer Support Center (IRSC) provides project management and support to credit unions implementing virtual channel projects such as MAP, Mobile App, MACO, credit union branding, and more.

The IRSC website brings together these digital strategy products in one location. If your credit union wants to expand its virtual channel marketplace, you can shop and explore the offerings online as well as check the status of initiatives as they are implemented.

Learn more in the IRSC website: https://irsc.cuanswers.com/

GETTING STARTED

Purchase in Store

Your first step to get started using Member Authentication Convenience Options (MACO) is to purchase the product in the CU*Answers online store. Purchasing MACO in the CU*Answers online store will alert the Internet Retailer Support Center (IRSC) that you are ready to offer MACO to your members.

https://irsc.cuanswers.com/product/maco-multiple-authentication-convenience-options/

Meet with IRSC Representative

Once you have purchased MACO, a representative from the IRSC will meet with you to go over the onboarding process and answer any additional questions you have. During this process you will sign a client agreement with CU*Answers.

How Many Licenses to Purchase

The IRSC will assist your credit with estimating the number of licenses your credit unions will need. Credit unions have the option to either purchase licenses in advance of use or to "true up" at the end of the calendar year. (There is a slight decrease in price for those purchases ahead of use.) Licenses are per calendar year. No partial credit is applied.

Customize User Agreement

The IRSC will provide your credit union with standard text of the MACO User Agreement. Your credit union may elect to customize this User Agreement due to state requirements or individual needs of your credit union. The customized text is appended to the end of the standard agreement text. During this step your credit union must sign off on approved text for the User Agreement.

- The member is presented the MACO User Agreement the first time they enroll in MACO. The member is presented this agreement again only when your credit union adjusts the text of the agreement, the member uses MACO on a different device, or if the member unenrolls completely from MACO and then uses it again.

Support of MACO

The IRSC will discuss support options for MACO. While your credit union will be the first line of support for member's questions, the IRSC can provide Tier 2 support.

CREDIT UNION FREQUENTLY-ASKED QUESTIONS (FAQ)

As you prepare to rollout a mobile application with MACO enabled, your staff should be prepared to address member who have issues, questions, or concern. This document/site is a resource that will provide some questions and answers to ensure you are given the best quality of service.

Question. 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.

Question: Which MACO option is the most secure

Answer: *No single authentication option should be looked at as being more secure than the others. Ultimately it comes down to the member's own usage and their environment. For example, if the 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. Your credit union should refrain from recommending any MACO on the basis of security, and explain that these options are a balance of security and convenience.*

Question: I have multiple accounts at the credit union. How do I get MACO to work with all my accounts?

Answer: You will only be able to use MACO to log on to one of your accounts per device.

Question: 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.

Question: 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.

Question: 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.

Question: 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.")

Question: 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.

Question: Can I select my own phrase when enrolling/using the voice authentication

No, personalized phrases are not supported.

Question: 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.

Question: 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.

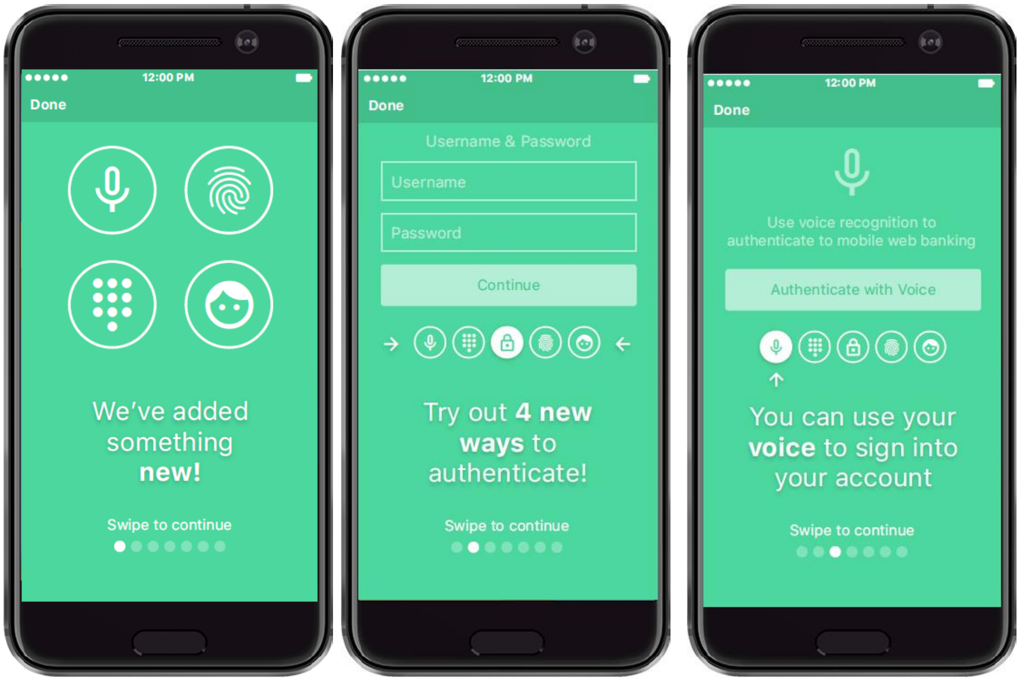
Enrollment and Authentication

This section covers a summary of what the member sees when enrolling in MACO and using MACO to authenticate for Mobile App Banking.

"We've Added Something New" Page

The member views these pages the first time they enter Mobile App after you activate the feature. The member can also revisit these pages in the Settings & Info section once they have logged on to Mobile App Banking.

The first time the member accesses Mobile Banking after your credit union activates MACO, they will see the "We've Added Something New" pages. The member scrolls right to learn more about each MACO. The member can begin enrollment from these pages or they can just serve as advertisement.



12:00 PM

Done

We've added something **new!**

Swipe to continue

12:00 PM

Done

Username & Password

Username

Password

Continue

Try out **4 new ways** to authenticate!

Swipe to continue

12:00 PM

Done

Use voice recognition to authenticate to mobile web banking

Authenticate with Voice

You can use your **voice** to sign into your account

Swipe to continue

All four authentication methods have their own promotion page; however, in the example above only the screen for fingerprint is shown. If the member's device does not support fingerprint authentication (or any other authentication method), the corresponding page will not be presented.

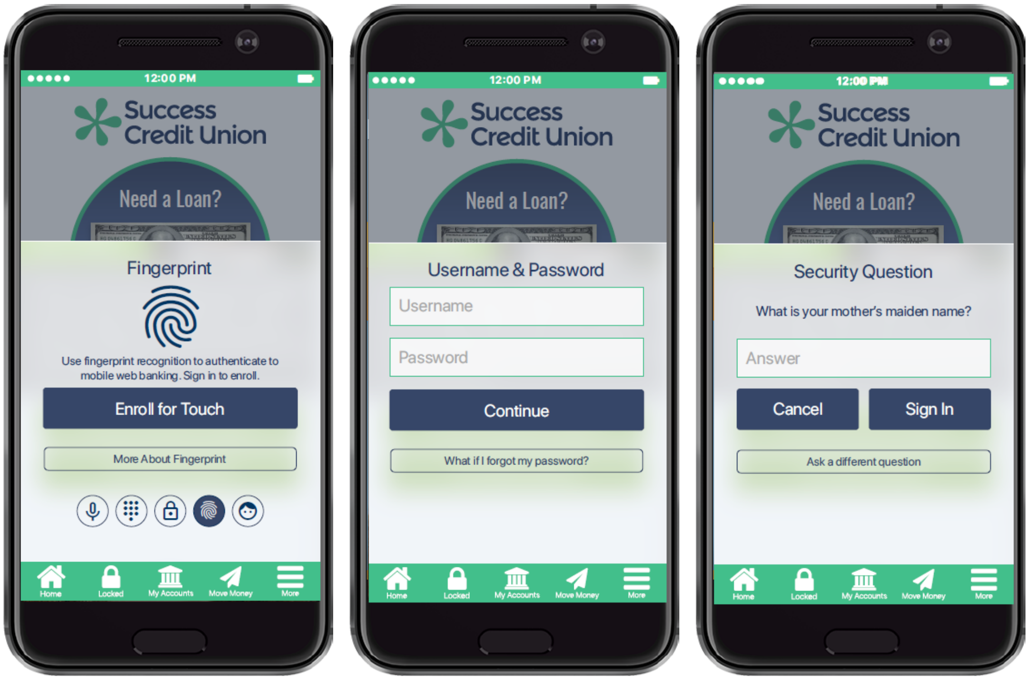
FINGERPRINT

Fingerprint Overview

Before starting fingerprint enrollment, the member must first save a fingerprint sample in the operating system of the device.

As stated earlier in this document, during fingerprint enrollment, the sensor on the device captures a fingerprint sample that is compared with the fingerprint saved on the device. If the fingerprint is a match, it is used for authentication. To authenticate, the member touches the sensor with their finger. If it is a match with the sample saved in the operating system, the member is logged on to Mobile App Banking.

Fingerprint Enrollment



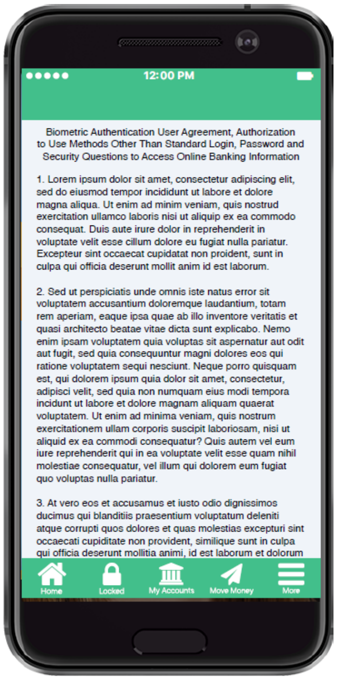
Use fingerprint recognition to authenticate to mobile web banking. Sign in to enroll.

What is your mother's maiden name?

To enroll, the member taps the MACO fingerprint icon at the bottom of the login screen and taps "Enroll for Touch."

The member authenticates with the standard authentication and enters their username, password, and a security question answer. The member taps "Sign In."

Fingerprint Enrollment (cont.)

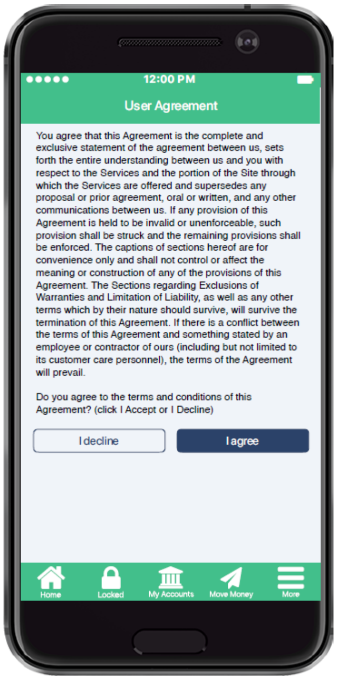


Biometric Authentication User Agreement, Authorization to Use Methods Other Than Standard Login, Password and Security Questions to Access Online Banking Information

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

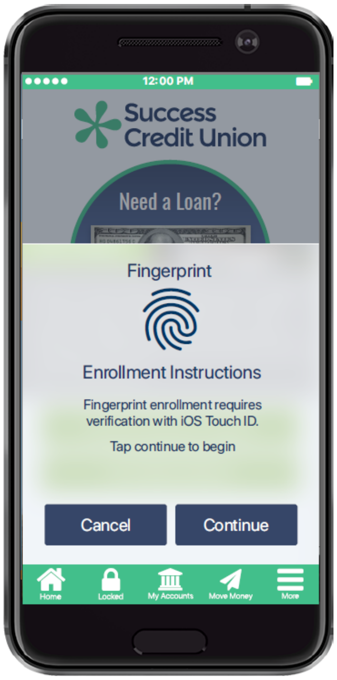
2. Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur.

3. At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum



You agree that this Agreement is the complete and exclusive statement of the agreement between us, sets forth the entire understanding between us and you with respect to the Services and the portion of the Site through which the Services are offered and supersedes any proposal or prior agreement, oral or written, and any other communications between us. If any provision of this Agreement is held to be invalid or unenforceable, such provision shall be struck and the remaining provisions shall be enforced. The captions of sections hereof are for convenience only and shall not control or affect the meaning or construction of any of the provisions of this Agreement. The Sections regarding Exclusions of Warranties and Limitation of Liability, as well as any other terms which by their nature should survive, will survive the termination of this Agreement. If there is a conflict between the terms of this Agreement and something stated by an employee or contractor of ours (including but not limited to its customer care personnel), the terms of the Agreement will prevail.

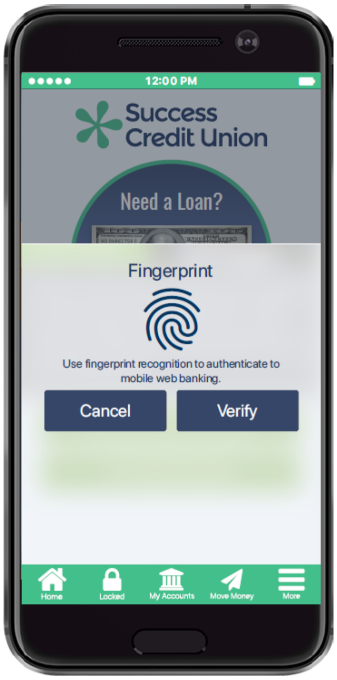
Do you agree to the terms and conditions of this Agreement? (click I Accept or I Decline)



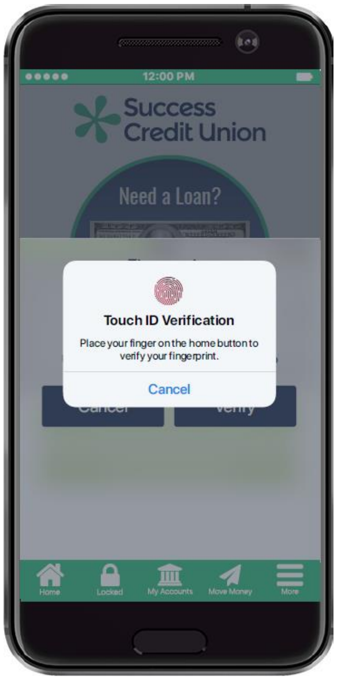
Fingerprint enrollment requires verification with iOS Touch ID.

Tap continue to begin

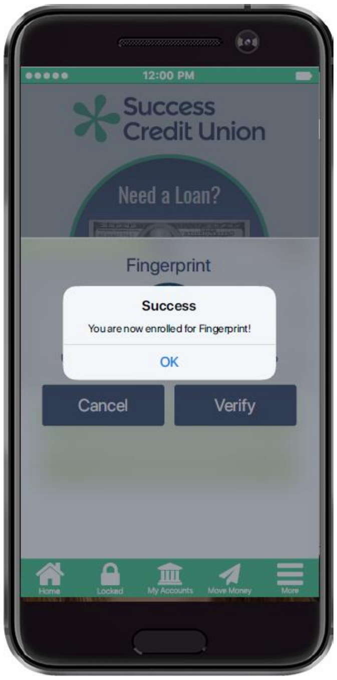
If the member hasn't already accepted the MACO User Agreement, it is presented for acceptance. The member scrolls to the end, and clicks "I agree." The member taps "Continue" to proceed.



Use fingerprint recognition to authenticate to mobile web banking.



Place your finger on the home button to verify your fingerprint.

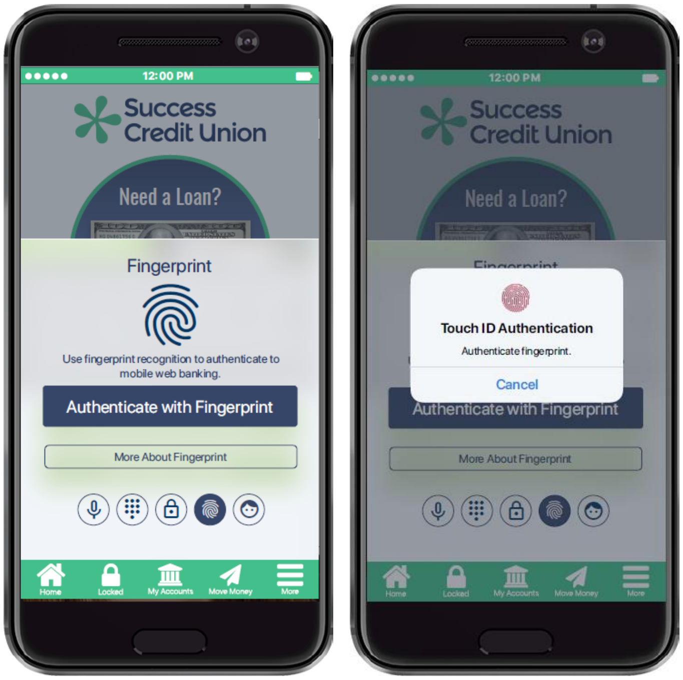


You are now enrolled for Fingerprint!

The member taps "Verify" and sees the touch ID verification sensor image. Messaging indicates the member should repeatedly touch the sensor of the device (for example the Home button). When the fingerprint sample collected is a match with the fingerprint sample saved in operating system of the device, the member sees the "Success" message.

The member taps "OK and is prompted to immediately authenticate with fingerprint for the first time. These steps are included in the next section.

Fingerprint Authentication



Use fingerprint recognition to authenticate to mobile web banking.

Authenticate fingerprint.

The member taps “Authenticate with Fingerprint,” and the touch ID authentication sensor graphic appears. The member touches the sensor on the device (for example the Home button) to verify against the fingerprint saved in the device operating system.

If there is a match, the member is logged on to Mobile App Banking and advances to the Home Page.

If the fingerprint fails to match, the touch ID sensor shakes, and the member touches the sensor to try to make a match. After three failed attempts, the member sees the “Try Again” message. The member clicks “OK” and can try to authenticate again.

Now fingerprint authentication is the default. The next authentication will move directly to the first screen show above. *The member can also configure their device to skip this step and move directly to the second screen where they place their finger on their device. Learn more about 1-Click Login on page 28.*

Members can always authenticate using another MACO or the standard login of username, password and security question.

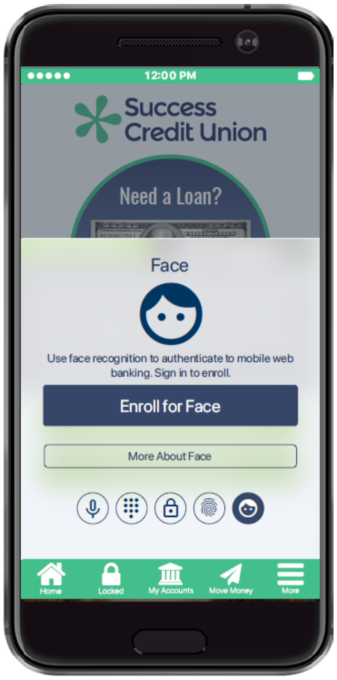
FACE RECOGNITION

Face Recognition Overview

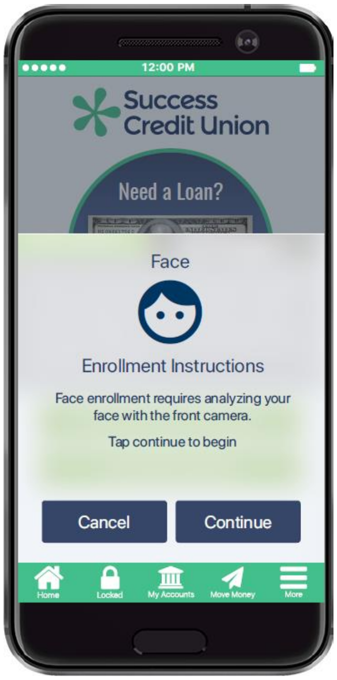
As stated earlier in this document, face recognition uses the camera of the device to capture photos of the member. The photos analyzed for quality, and an encrypted metric assigned to the best photo is sent to the DAON server. (The actual photo is not sent to DAON.)

During authentication, the member nods (or blinks or shakes) and the app uses the camera of the device to take a "live check" picture of the member. If this photo's metric matches what is saved on the DAON server, the member is logged on to Mobile App Banking.

Face Recognition Enrollment



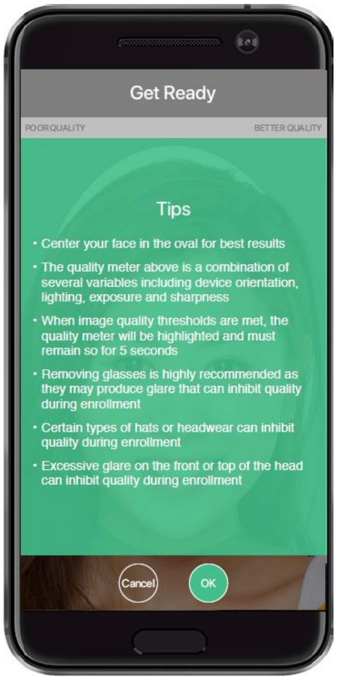
Use face recognition to authenticate to mobile web banking. Sign in to enroll.



Enrollment Instructions

Face enrollment requires analyzing your face with the front camera.

Tap continue to begin



Tips

- Center your face in the oval for best results
- The quality meter above is a combination of several variables including device orientation, lighting, exposure and sharpness
- When image quality thresholds are met, the quality meter will be highlighted and must remain so for 5 seconds
- Removing glasses is highly recommended as they may produce glare that can inhibit quality during enrollment
- Certain types of hats or headwear can inhibit quality during enrollment
- Excessive glare on the front or top of the head can inhibit quality during enrollment

The member taps the MACO face icon at the bottom of the login pane and taps "Enroll for Face."

- The member is prompted to authenticate using their standard authentication of username, password and security question answer. If the member hasn't already accepted the MACO User Agreement, it is presented for acceptance. *This is not shown in this section. Refer to the "Enroll in Fingerprint" section of this booklet on page 10.)*

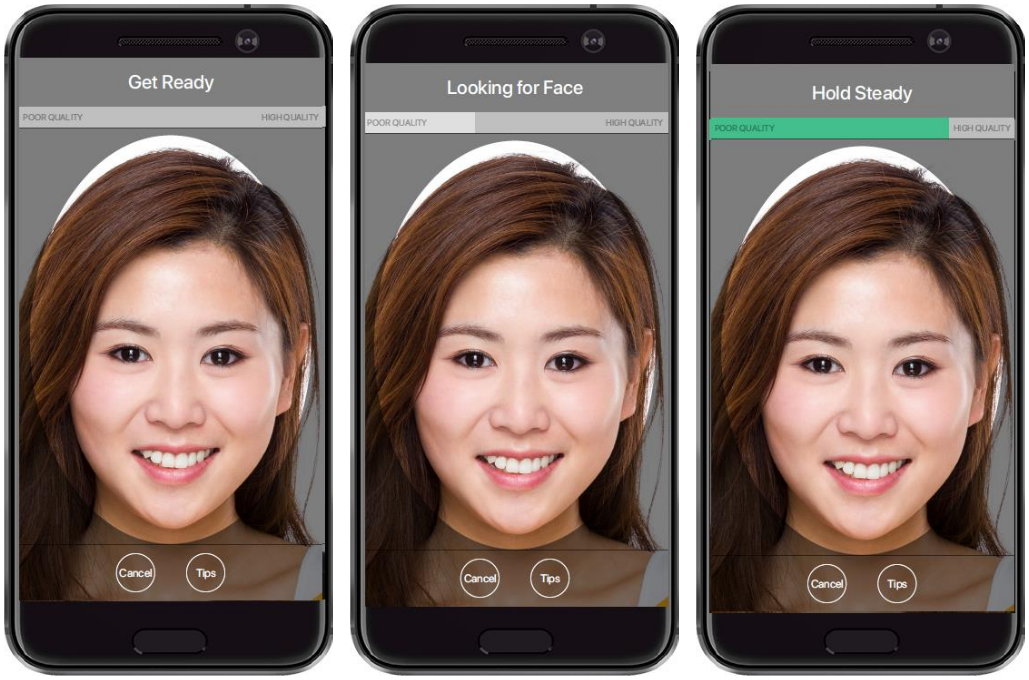
The member taps "Continue." *At this point MACO may ask for access to the device camera.*

The member then views helpful tips on the face recognition enrollment process. This includes recommendations to avoid excessive glare and to remove glasses and hats.

NOTE: A front-facing camera is required for face recognition enrollment and authentication.

To advance, the member taps "OK."

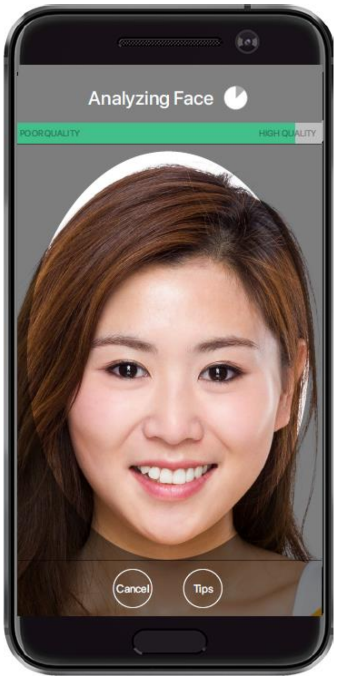
Face Enrollment (cont.)

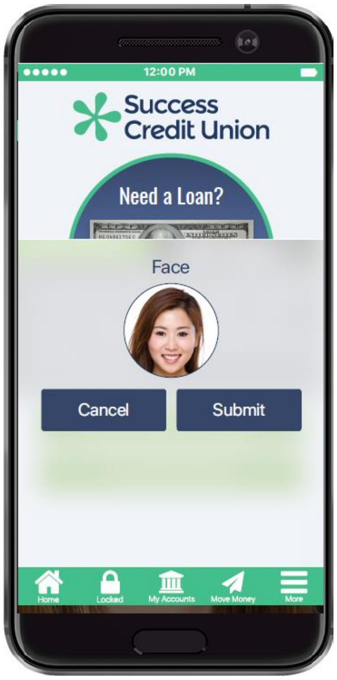


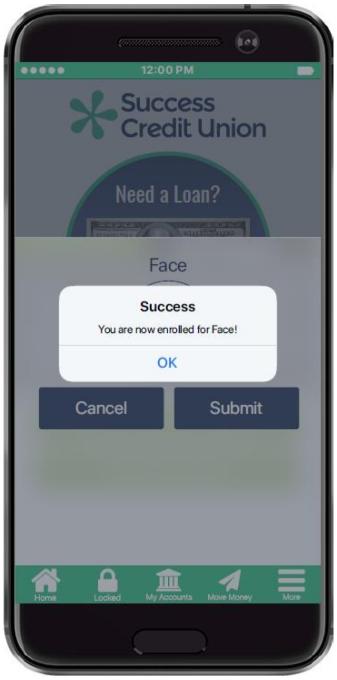
The member sees messaging at the top of the device that helps them position the camera to capture a successful photo. The Quality meter at the top of the screen changes color to indicate the quality of the image.

- First the member sees “Get Ready.”
- While the member positions the camera correctly, the member sees “Looking for Face.”
    - *If the member is not holding the device vertically, the messaging changes to “Hold Device Upright.” This is not shown above.*
- When the camera is ready to take pictures, the member is prompted to “Hold Steady.”

Face Enrollment (cont.)







Success

You are now enrolled for Face!

When the quality meter hits an acceptable range, the member sees “Analyzing Face,” and the camera begins taking pictures.

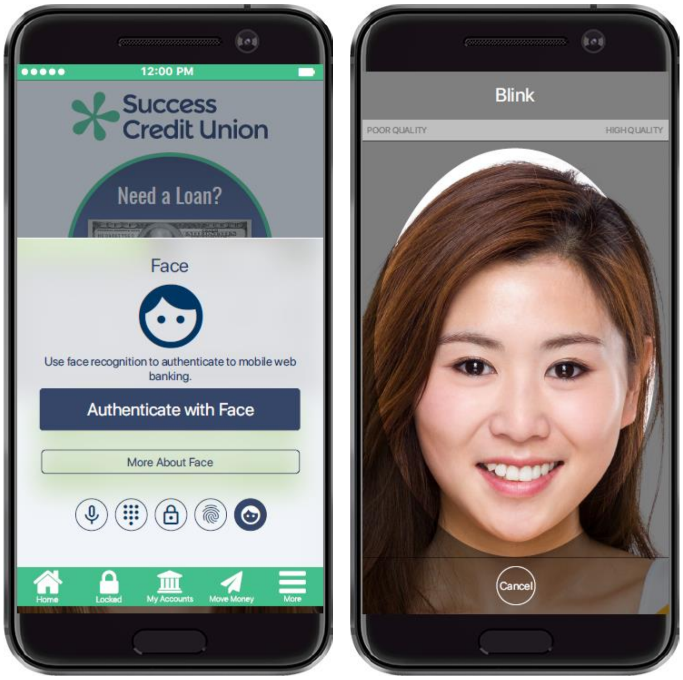
The best picture is presented in the window. To accept it, the member taps “Submit.” *To take a different photo, the member taps the picture, and the device takes another series of pictures. (If the member taps “Cancel” the member exits face recognition enrollment.)*

- If the captured picture doesn’t meet quality standards, the member sees “Try Again” (not shown). The member then taps “OK,” and repeats the photo capture process. (The member does not see the entry page tips again.)

When the photo submitted is of acceptable quality, the member sees “Success” and a metric of the photo is sent to the DAON server. (No actual photo is sent.)

The member is prompted to tap “OK” to advance to authenticate with face recognition for the first time. This is covered in the next section.

Face Recognition Authentication



Use face recognition to authenticate to mobile web banking.

The member taps “Authenticate with Face,” and the camera from the device opens. The member sees “Looking for Face” (not shown).

When a face is detected, the member sees “Blink.” The member blinks to confirms that the camera is taking a “live” photo.

- *Blink is the default. Nod and shake are other liveness options. This setting can be changed in Setting & Info. See page 28.*

If the captured photo matches the photo metric saved on the DAON server, the member is logged in to Mobile App Banking and unlocks the Mobile App.

If the quality of the picture is not adequate or the picture is not a match, the member is prompted to tap “Try Again.” This causes the camera to reappear to take another photo.

Now face recognition authentication is the default. The next authentication will move directly to the first screen show above. *The member can also configure their device to skip this step and move directly the screen where the camera takes their picture. Learn more about 1-Click Login on page 28.*

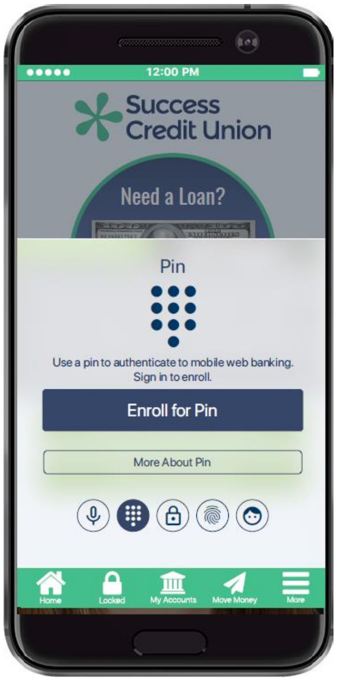
Members can always authenticate using another MACO or the standard login of username, password and security question.

Personal Identification Number (PIN)

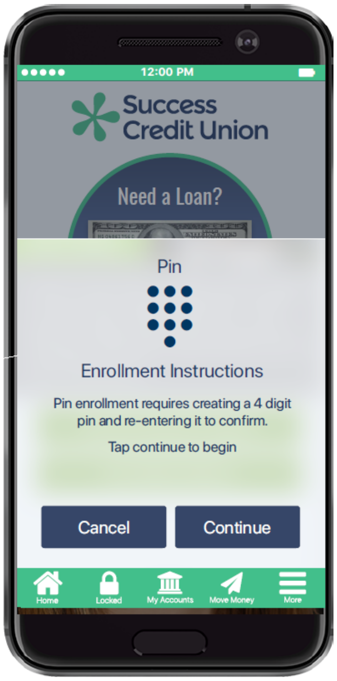
PIN Overview

As stated earlier in this document, PIN enrollment captures a four-digit PIN and then uses this PIN for authentication.

PIN Enrollment



Use a pin to authenticate to mobile web banking. Sign in to enroll.



Pin enrollment requires creating a 4 digit pin and re-entering it to confirm.

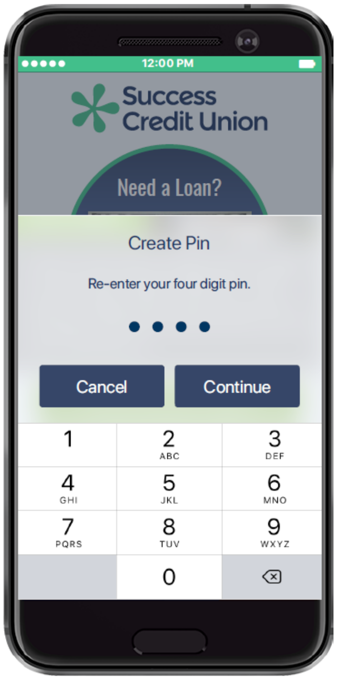
Tap continue to begin

The member taps the MACO PIN icon at the bottom of the login pane and taps "Enroll for Pin."

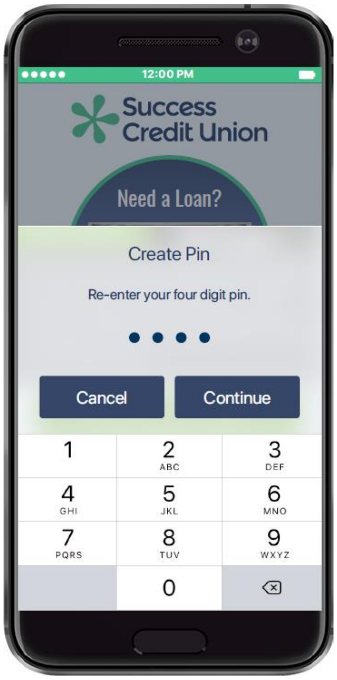
- The member is prompted to authenticate using their standard authentication of username, password and security question answer. If the member hasn't already accepted the MACO User Agreement, it is presented for acceptance. *This is not shown in this section. Refer to the "Enroll in Fingerprint" section of this booklet on page 10.)*

The member then taps "Continue" to proceed.

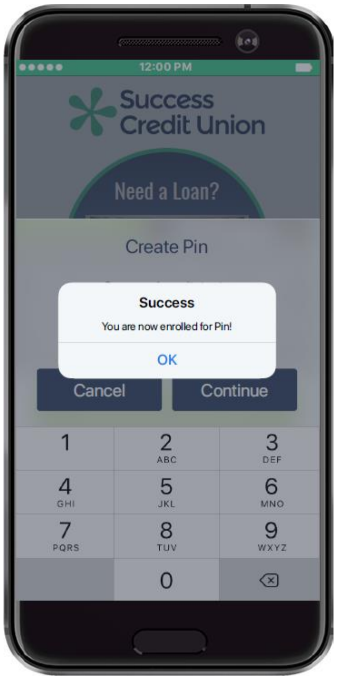
PIN Enrollment (cont.)


Create Pin

Re-enter your four digit pin.


Create Pin

Re-enter your four digit pin.

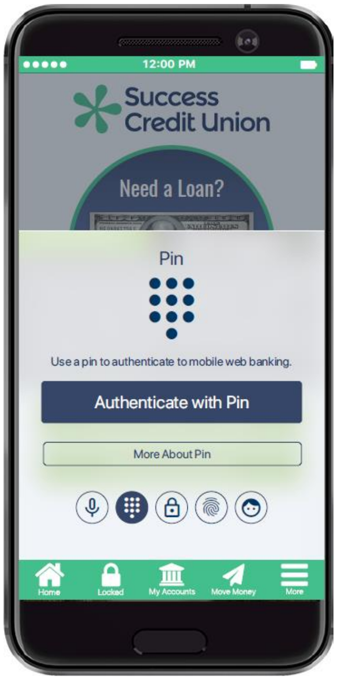

Create Pin

Success

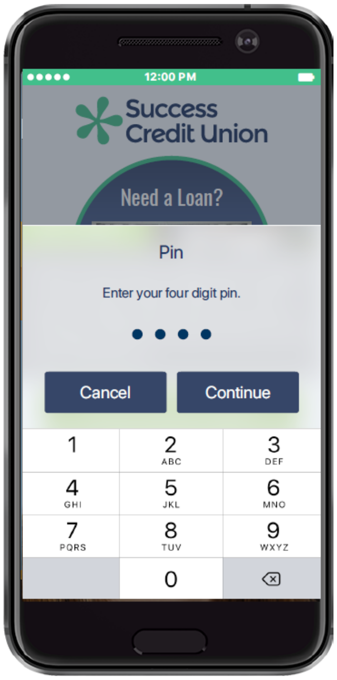
You are now enrolled for Pin!

The member is prompted to enter and re-enter a four-digit PIN in the number pad provided on the screen. When there is a match, the member sees "Success." The member taps "OK" to advance and authenticate with PIN for the first time. This is covered in the next section.

PIN Authentication


Pin

Use a pin to authenticate to mobile web banking.


Pin

Enter your four digit pin.

The member taps "Authenticate with Pin," and the number pad appears. The member is prompted to enter and re-enter their four-digit PIN. When the correct PIN is entered twice, the member is logged in to Mobile App Banking and advances to the Home Page.

PIN Authentication (cont.)

If the PINs do not match, the member is prompted to "Try Again." The member clicks "OK" and the number pad is presented again.

Now PIN authentication is the default. The next authentication will move directly to the first authentication screen shown on the previous page. *The member can also configure their device to skip this step and move directly to the second screen where they enter their PIN. Learn more about 1-Click Login on page 28.*

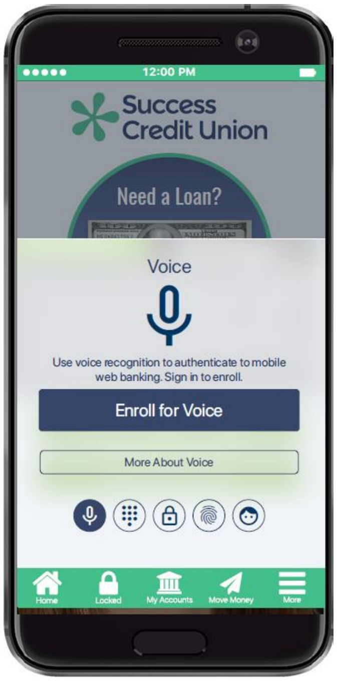
Members can always authenticate using another MACO or the standard login of username, password and security question.

VOICE RECOGNITION

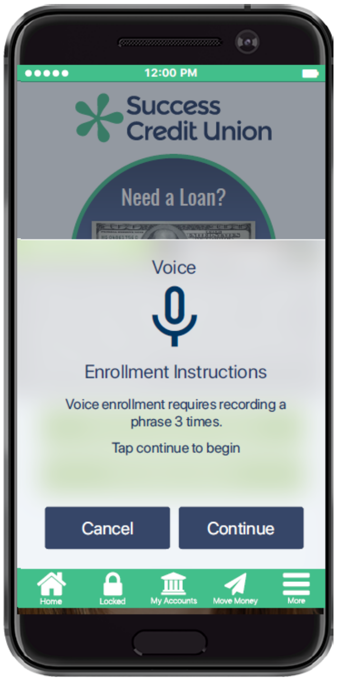
Voice Recognition Overview

As stated earlier in this document, during voice recognition enrollment, the member recites a passphrase until they have three successful recordings. The best recording is converted to voice data which is saved on the DAON server. (No voice recording is saved.) During authentication, the member recites the phrase again. If this voice data matches what is saved on the DAON server, the member is logged on to Mobile App Banking.

Voice Recognition Enrollment



Use voice recognition to authenticate to mobile web banking. Sign in to enroll.



Enrollment Instructions

Voice enrollment requires recording a phrase 3 times.

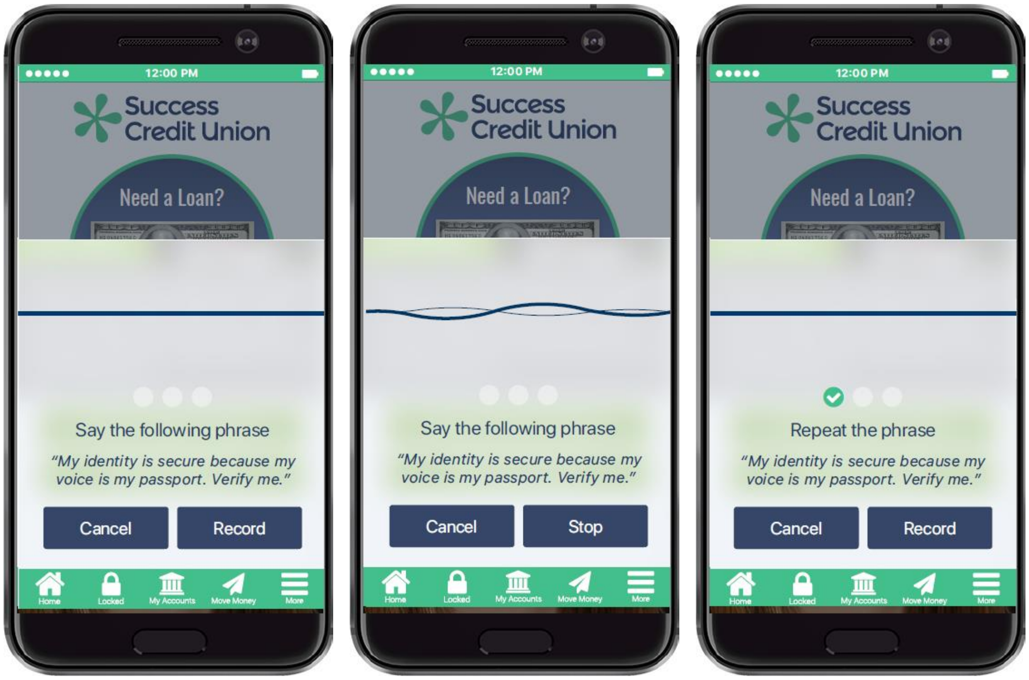
Tap continue to begin

The member taps the MACO microphone icon at the bottom of the login pane and taps "Enroll for Voice."

- The member is prompted to authenticate using their standard authentication of username, password and security question answer. If the member hasn't already accepted the MACO User Agreement, it is presented for acceptance. *This is not shown in this section. Refer to the "Enroll in Fingerprint" section of this booklet on page 10.)*

The member taps "Continue" to proceed. *At this point MACO may ask for access to the device microphone.*

Voice Enrollment (cont.)



Say the following phrase

"My identity is secure because my voice is my passport. Verify me."

Say the following phrase

"My identity is secure because my voice is my passport. Verify me."

Repeat the phrase

"My identity is secure because my voice is my passport. Verify me."

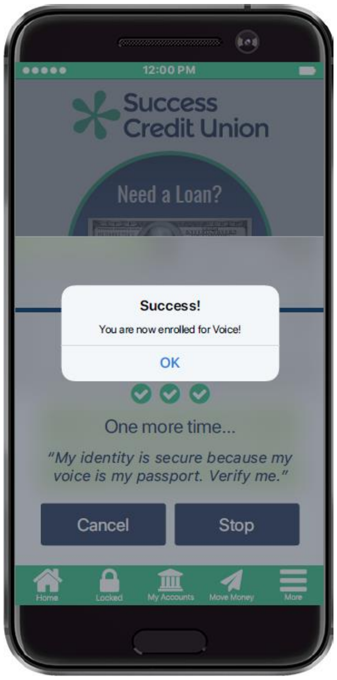
The member sees the passphrase and is instructed to say it. The member taps "Record," says the phrase, and taps "Stop."

- As the member says the phrase, a visible waveform appears on the screen.

If the recording is of an acceptable quality, a check appears on the screen.

If the recording does not meet quality standards, the member sees, "Try Again. Audio quality is insufficient." The member clicks "OK" and recites the phrase again.

Voice Enrollment (cont.)



Success!

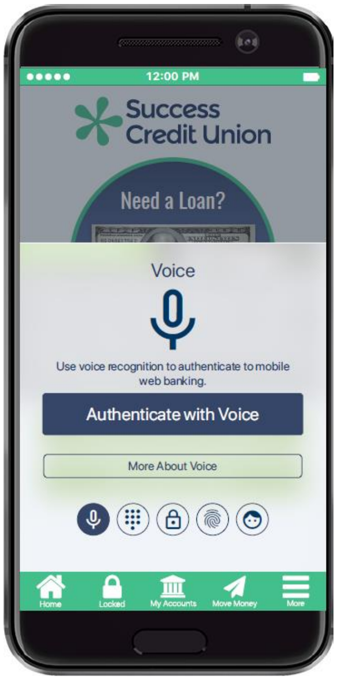
You are now enrolled for Voice!

One more time...

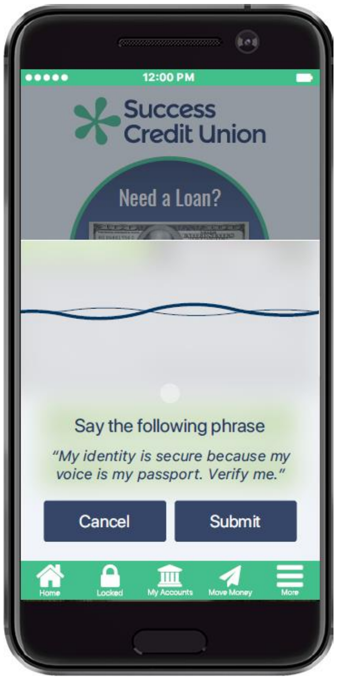
"My identity is secure because my voice is my passport. Verify me."

The member repeats this process until three readings are accepted and three checkmarks appear on the screen. At this point, the "Success" message is displayed. The member taps "OK" and advances to authenticate with their voice for the first time. This is covered in the next section.

Voice Authentication



Use voice recognition to authenticate to mobile web banking.



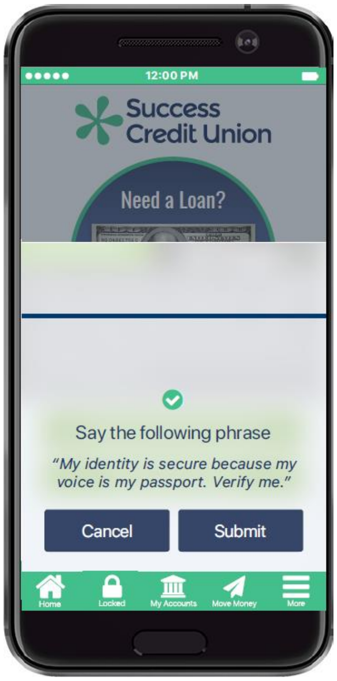
Say the following phrase

"My identity is secure because my voice is my passport. Verify me."

The member taps "Authenticate with Voice," and the member is presented the passphrase. The member says the phrase and sees a visible wave on the screen. When the phrase is of acceptable quality, the member sees a check on the screen (shown on next page).

Voice Authentication (cont.)

If the phrase does not meet quality standards, the member is told, "Try again. Audio quality is insufficient." The member taps "OK" and tries again.

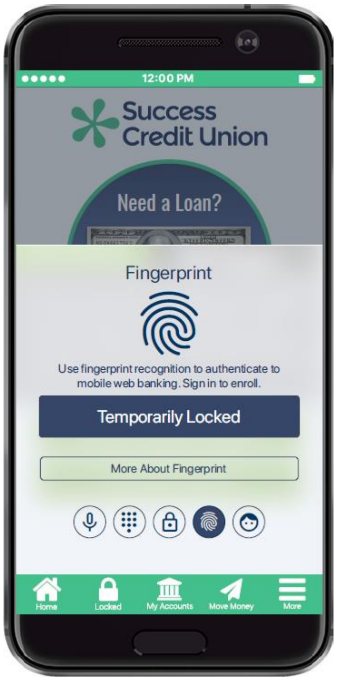


The member taps "Submit." The audio data is sent to DAON for a match. (No recording is sent.) If a successful match is made, the member is logged on to Mobile App Banking and advances to the Home Page.

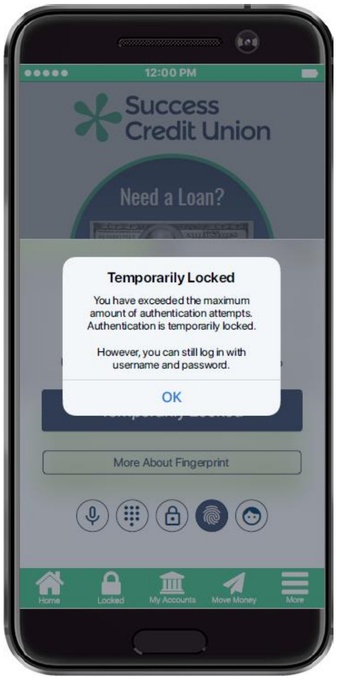
Now voice recognition authentication is the default. The next authentication will move directly to the first authentication screen shown on the previous page. *The member can also configure their device to skip this step and move directly to the second screen where they say the phrase. Learn more about 1-Click Login on page 28.*

Members can always authenticate using another MACO or the standard login of username, password and security question.

TEMPORARY LOCKOUT



Use fingerprint recognition to authenticate to mobile web banking. Sign in to enroll.



Temporarily Locked

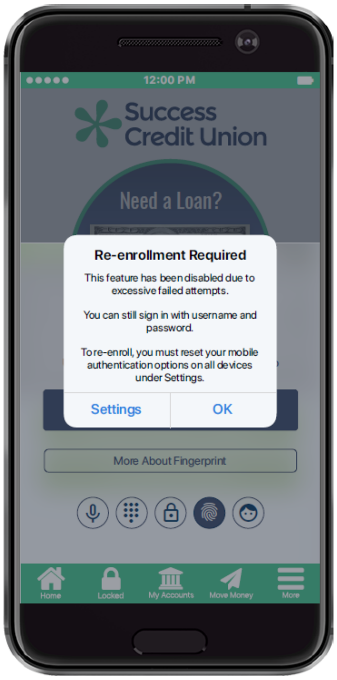
You have exceeded the maximum amount of authentication attempts. Authentication is temporarily locked.

However, you can still log in with username and password.

After several failed MACO authentication attempts, the member will be temporarily locked out of authenticating with any MACO, regardless of which MACO authentication caused the lockout. The member clicks “Temporarily Locked,” to read a message stating that they have exceeded the allowed attempts and are temporarily locked. *They can still log in using the standard login of username and password.*

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

If a member fails to authenticate correctly several times, the member may also be asked to enter their device passcode.



Re-enrollment Required

This feature has been disabled due to excessive failed attempts.

You can still sign in with username and password.

To re-enroll, you must reset your mobile authentication options on all devices under Settings.

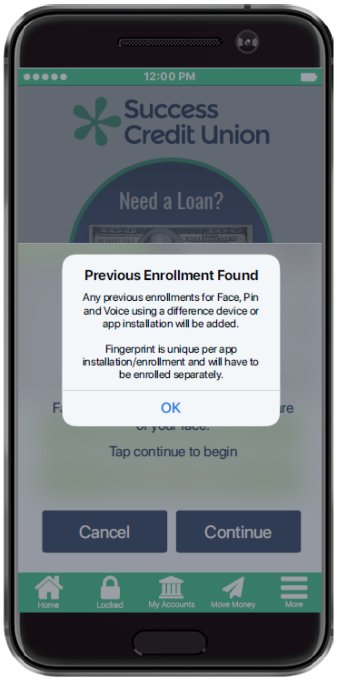
At the fourth lockout, the member’s MACO profile is disabled. This means they cannot authenticate using MACO on any device. The member sees a message saying that “Re-enrollment is required.”

To use MACO again, the member clicks “Settings” to go to the “Settings & Info” section of the Mobile App. (See page 25 for information on this section of the Mobile App.) In that area of the Mobile App, the member then uses “Reset Authentication Options on All Devices” to reset their profile. Then (still in Settings & Info), the member turns the switch for a MACO to the “on” position. This will allow them to re-enroll in the MACO. The member will be presented the MACO User Agreement during this authentication.

ONE MEMBERSHIP PER CREDIT UNION PER DEVICE

MACO only supports one membership per credit union per device.

Prior MACO Profile Found For Member



Previous Enrollment Found

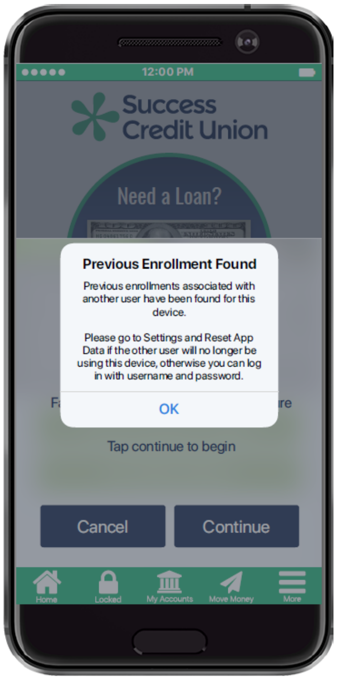
Any previous enrollments for Face, Pin and Voice using a difference device or app installation will be added.

Fingerprint is unique per app installation/enrollment and will have to be enrolled separately.

If the member attempts to enroll in MACO on a second device, the member is notified that an earlier MACO profile has been found.

The member is prompted to tap “OK” to copy the authentication enrollments to this second device.

Fingerprint setup is per device so the member will be prompted to set that up separately.



Previous Enrollment Found

Previous enrollments associated with another user have been found for this device.

Please go to Settings and Reset App Data if the other user will no longer be using this device, otherwise you can log in with username and password.

Another Member Has MACO Profile on Device

Only one face, voice or PIN MACO profile is allowed per device. *The number of fingerprint profiles supported is determined by the device.*

If MACO detects that another user has set up a MACO profile on the device previously, it will instruct the member to reset the device to clear the other user profile. (How to clear the profile is covered in on page 30 of this booklet.) The member taps “OK” to close the message.

This message might be seen when two people are sharing a device as well. As an example, let’s say a husband and wife are sharing a phone, and the husband has set up a face profile. The wife will see this message when she attempts to set up her face profile on the same device. *In this situation, it is possible for husband to use the face profile and the wife to use the voice profile. As mentioned above, the number of supported fingerprint profiles is determined by the device.*

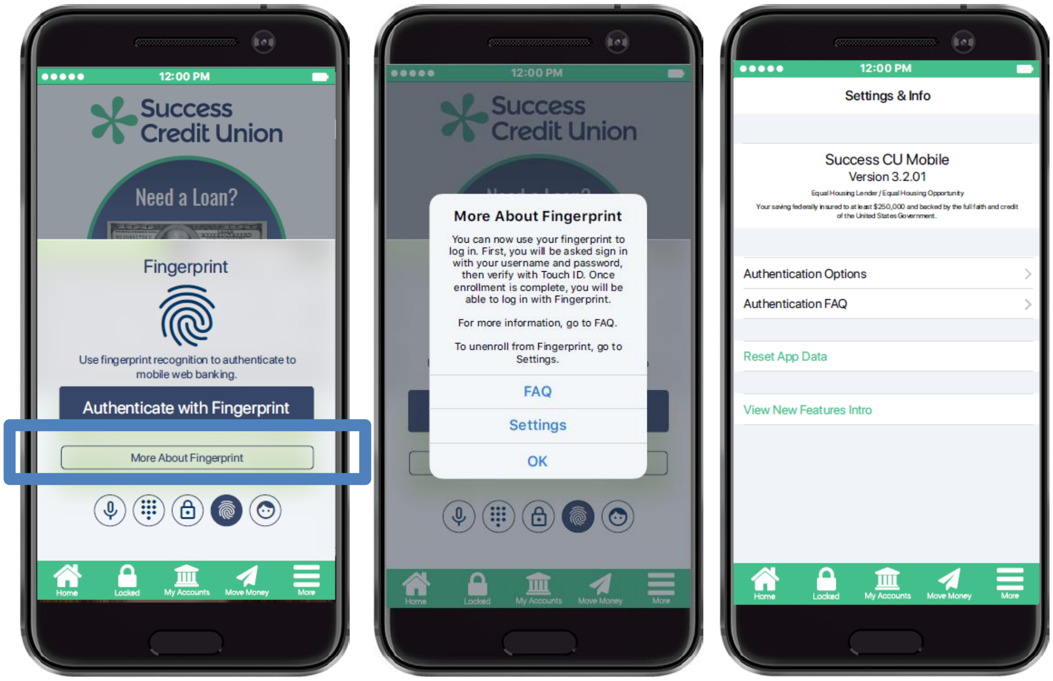
Features Accessed from Settings & Info

This section covers features accessed from the Settings & Info screen including: Quick Authentication, changing the face recognition liveness test options, unenrollment, and deactivation.

The Settings & Info screen provides the member with the version of the App they are using and access to Authentication Frequently-Asked Questions (FAQ) that are organized by authentication type.

Access to Settings & Info Screen

Access to Settings & Info via "More About"



Use fingerprint recognition to authenticate to mobile web banking.

More About Fingerprint

You can now use your fingerprint to log in. First, you will be asked sign in with your username and password, then verify with Touch ID. Once enrollment is complete, you will be able to log in with Fingerprint.

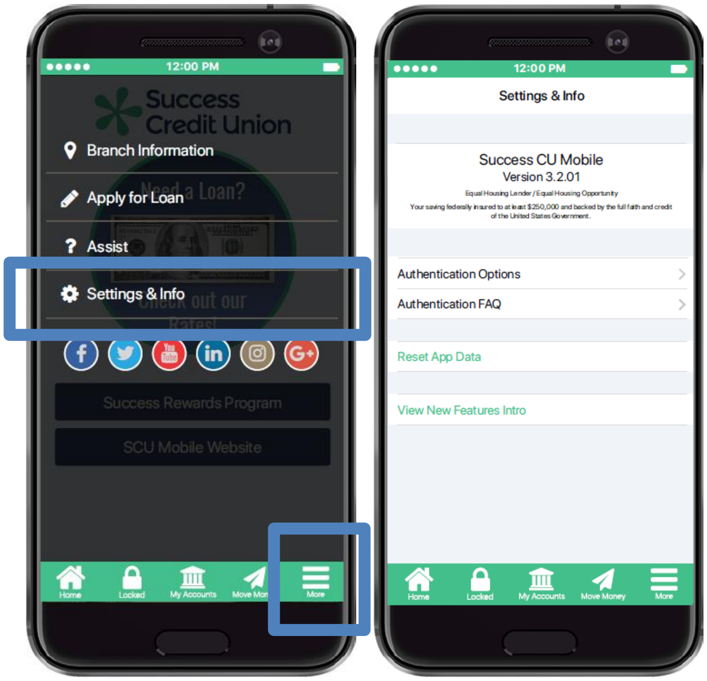
For more information, go to FAQ.

To unenroll from Fingerprint, go to Settings.

Success CU Mobile
Version 3.2.01
Equal Housing Lender / Equal Housing Opportunity
Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

From an authentication screen, the member taps "More About." Then on the popup window, the member taps "Settings."

Access to Settings & Info via the “More” Button



Equal Housing Lender / Equal Housing Opportunity

Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

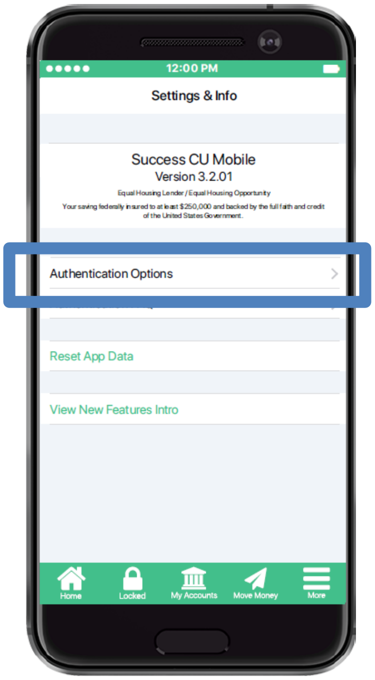
Alternatively, the member taps “More” at the bottom of the App and then taps “Settings & Info.”

Quick Authentication (1-Click Login)

Authentication always defaults to the last-used authentication. Members can skip the step where they click the “Authenticate with” button and instead automatically advance to the second login screen. For example, if the member uses fingerprint authentication to log on to Mobile App Banking and then activates this feature, the next time they log on, their device will automatically prompt them to place their finger on the device. (They will not have to first select the MACO to authenticate.)

Members can always elect to turn off Quick Authentication after they activate it. Then they can select to authenticate using any MACO (that they have enrolled in), or they can authenticate using the standard username, password, and security question answer.

Step-by-Step Directions


12:00 PM

Settings & Info

Success CU Mobile
Version 3.2.01

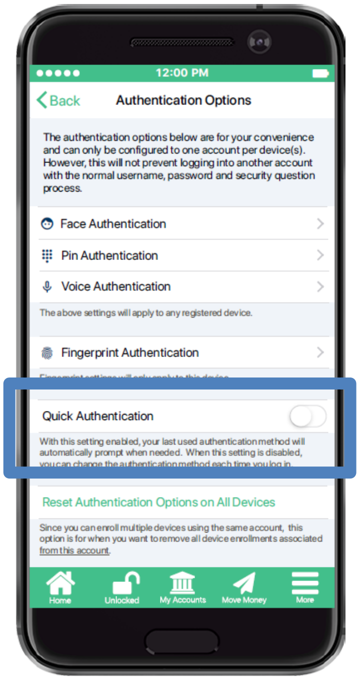
Equal Housing Lender / Equal Housing Opportunity

Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

Authentication Options

Reset App Data

View New Features Intro


12:00 PM

Back — Authentication Options

The authentication options below are for your convenience and can only be configured to one account per device(s). However, this will not prevent logging into another account with the normal username, password and security question process.

Face Authentication

Pin Authentication

Voice Authentication

The above settings will apply to any registered device.

Fingerprint Authentication

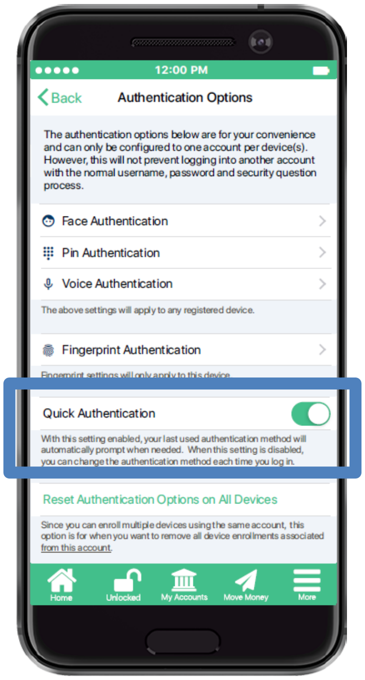
Fingerprint settings will only apply to this device.

Quick Authentication ○

With this setting enabled, your last used authentication method will automatically prompt when needed. When this setting is disabled, you can change the authentication method each time you log in.

Reset Authentication Options on All Devices

Since you can enroll multiple devices using the same account, this option is for when you want to remove all device enrollments associated from this account.


12:00 PM

Back — Authentication Options

The authentication options below are for your convenience and can only be configured to one account per device(s). However, this will not prevent logging into another account with the normal username, password and security question process.

Face Authentication

Pin Authentication

Voice Authentication

The above settings will apply to any registered device.

Fingerprint Authentication

Fingerprint settings will only apply to this device.

Quick Authentication ●

With this setting enabled, your last used authentication method will automatically prompt when needed. When this setting is disabled, you can change the authentication method each time you log in.

Reset Authentication Options on All Devices

Since you can enroll multiple devices using the same account, this option is for when you want to remove all device enrollments associated from this account.

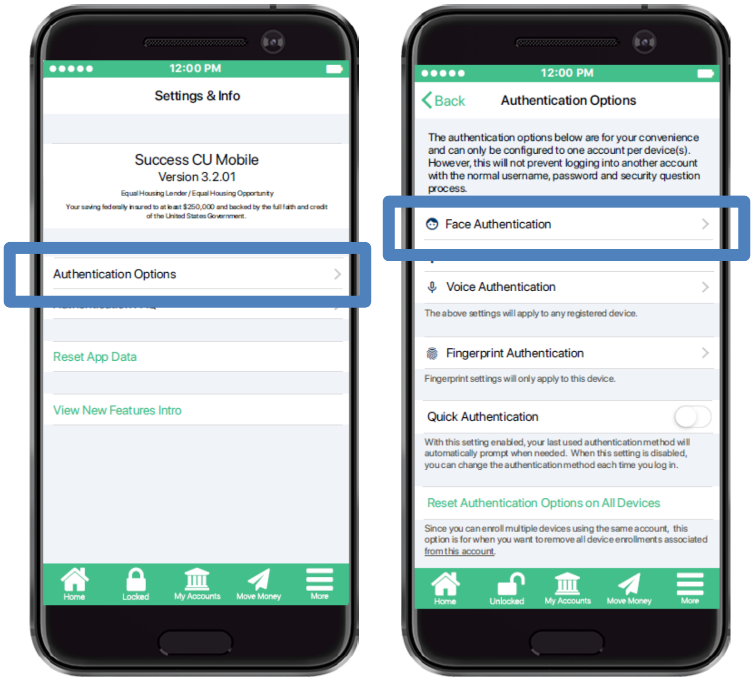
To activate Quick Authentication, the member taps “Authentication Options” on the Settings & Info screen. From there the member taps the switch next to “Quick Authentication” to the active (colored) position.

To disable Quick Authentication, the member taps the switch to turn it to the inactive (white) position.

Changing the Face Recognition Action (Blink, Nod, and Shake)

The default for face recognition authentication is for the member to nod their head to capture the photo. This provides the “liveness” test. Other “liveness” options include having the member nod or shake their head. The member can select an alternate motion test from the Settings & Info screen.

Step-by-Step Directions



Settings & Info

Success CU Mobile
Version 3.2.01
Equal Housing Lender / Equal Housing Opportunity
Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

Authentication Options >

Reset App Data

View New Features Intro

< Back Authentication Options

The authentication options below are for your convenience and can only be configured to one account per device(s). However, this will not prevent logging into another account with the normal username, password and security question process.

Face Authentication >

Voice Authentication >

The above settings will apply to any registered device.

Fingerprint Authentication >

Fingerprint settings will only apply to this device.

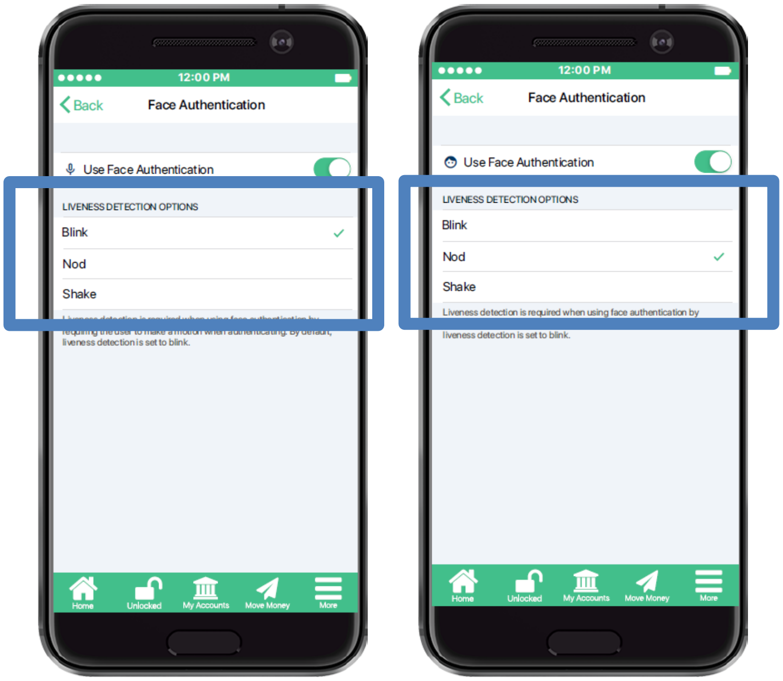
Quick Authentication ○

With this setting enabled, your last used authentication method will automatically prompt when needed. When this setting is disabled, you can change the authentication method each time you log in.

Reset Authentication Options on All Devices

Since you can enroll multiple devices using the same account, this option is for when you want to remove all device enrollments associated from this account.

The member taps “Authentication Options” and then “Face Authentication.”



< Back Face Authentication

Use Face Authentication ●

LIVENESS DETECTION OPTIONS

Blink ✓

Nod

Shake

liveness detection is set to blink.

< Back Face Authentication

Use Face Authentication ●

LIVENESS DETECTION OPTIONS

Blink

Nod ✓

Shake

Liveness detection is required when using face authentication by

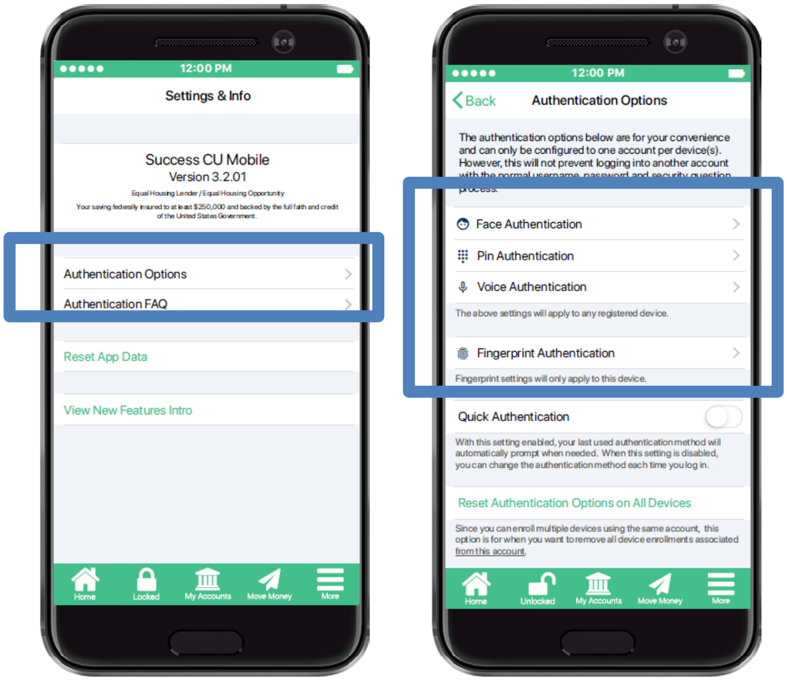
liveness detection is set to blink.

From the Face Authentication screen, the member taps to move the colored checkmark next to the desired liveness detection option. *In the example above “Nod” is selected instead of “Blink.”*

Unenrollment

These directions are used to unenroll from one MACO at a time. To use the MACO again, the member must re-enroll.

Step-by-Step Directions



12:00 PM

Settings & Info

Success CU Mobile
Version 3.2.01

Equal Housing Lender / Equal Housing Opportunity

Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

Authentication Options

Authentication FAQ

Reset App Data

View New Features Intro

12:00 PM

Back

Authentication Options

The authentication options below are for your convenience and can only be configured to one account per device(s). However, this will not prevent logging into another account with the normal username, password and security question process.

Face Authentication

Pin Authentication

Voice Authentication

The above settings will apply to any registered device.

Fingerprint Authentication

Fingerprint settings will only apply to this device.

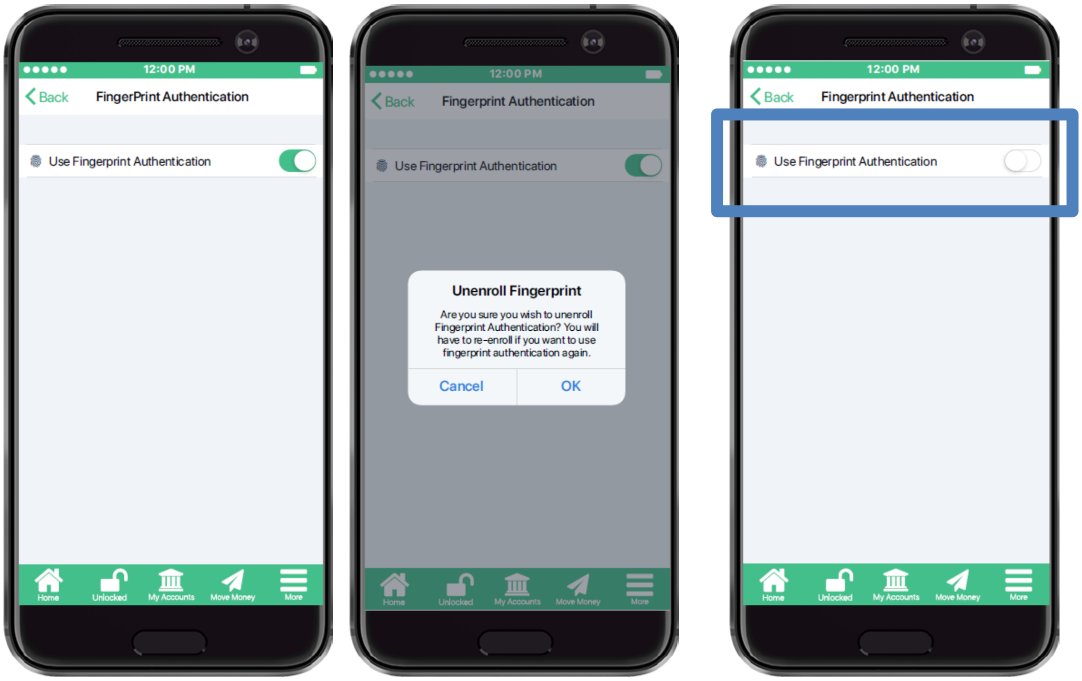
Quick Authentication

With this setting enabled, your last used authentication method will automatically prompt when needed. When this setting is disabled, you can change the authentication method each time you log in.

Reset Authentication Options on All Devices

Since you can enroll multiple devices using the same account, this option is for when you want to remove all device enrollments associated from this account.

From the Settings & Info screen, the member taps “Authentication Options” and then the MACO from which they want to unenroll.



12:00 PM

Back

FingerPrint Authentication

Use Fingerprint Authentication

12:00 PM

Back

Fingerprint Authentication

Use Fingerprint Authentication

Unenroll Fingerprint

Are you sure you wish to unenroll Fingerprint Authentication? You will have to re-enroll if you want to use fingerprint authentication again.

Cancel

OK

12:00 PM

Back

Fingerprint Authentication

Use Fingerprint Authentication

Then the member taps the colored activation switch to move it to the off (non-colored) position. The member clicks “OK” on the confirmation screen, and the MACO is disabled.

The example on the previous page shows fingerprint unenrollment; however, these steps can be used to deactivate any MACO.

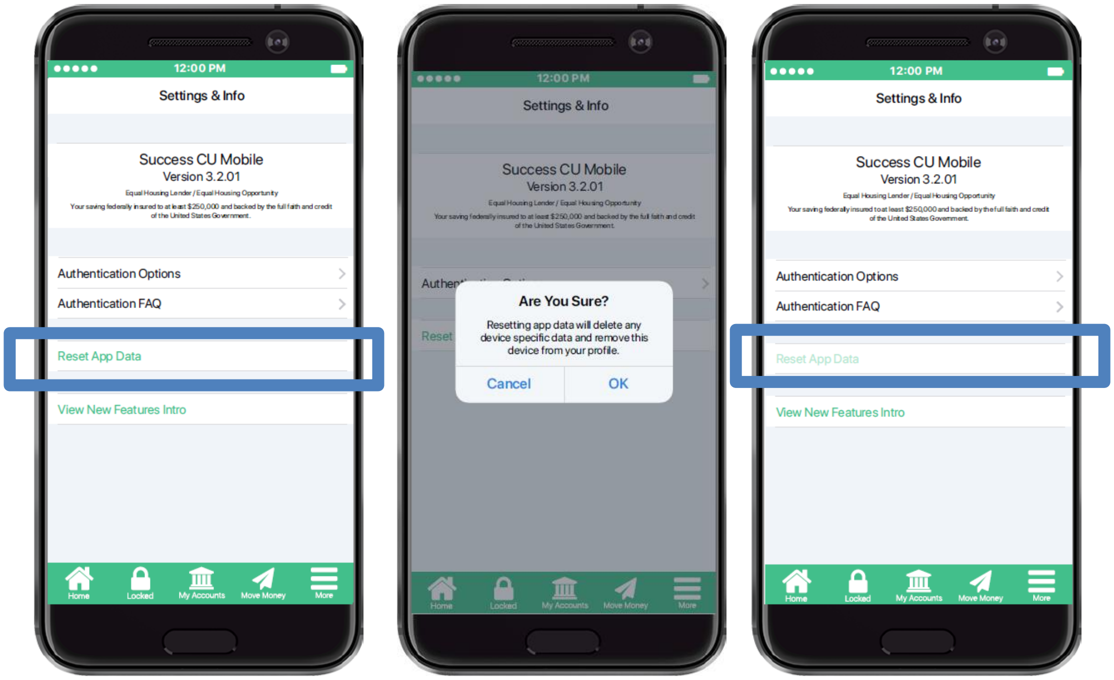
To use this MACO again, the member must re-enroll in it.

Remove MACO Profile from Device

The member may wish to deactivate all MACO enrollments on their device. Their MACO profile that is housed on the DAON server is then removed from the device. After the member completes this process, they cannot use any MACO to authenticate on this device. If they wish to use MACO again on this device, they must re-enroll.

These directions are also used if another profile is found on the device and the member wishes to clear the existing profile so that they can copy their own profile to the device. (Only one MACO profile is allowed per device.)

Step-by-Step Directions



Success CU Mobile
Version 3.2.01
Equal Housing Lender / Equal Housing Opportunity
Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

Are You Sure?
Resetting app data will delete any device specific data and remove this device from your profile.

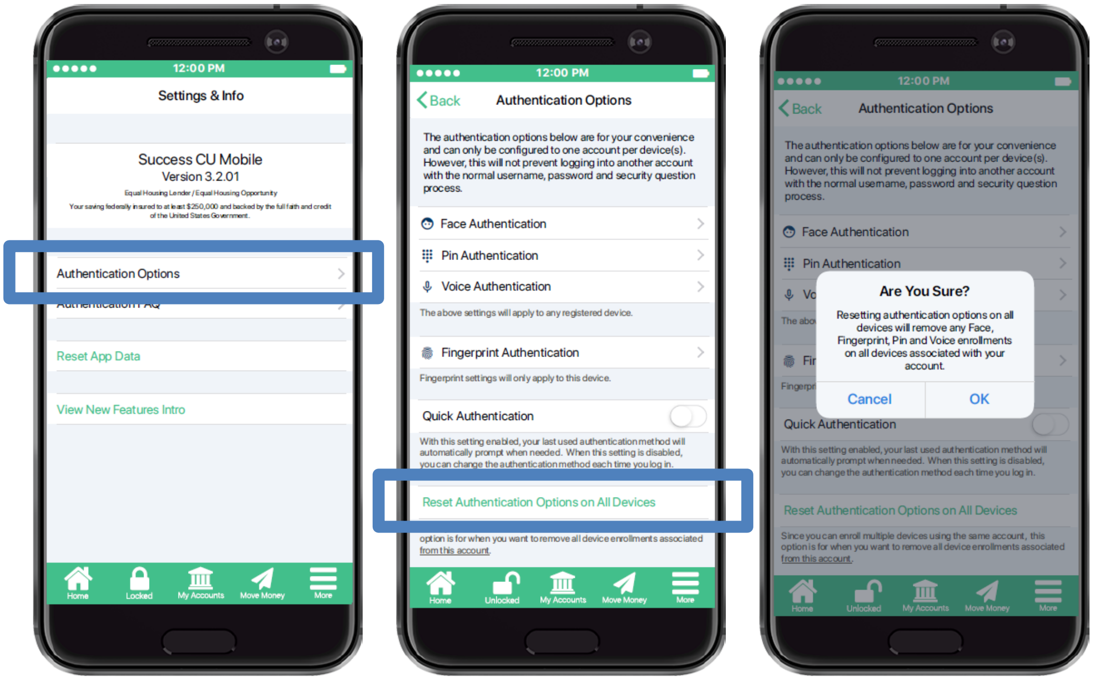
To remove the MACO profile from the device, the member taps “Reset App Data” on the Settings & Info screen. The member then taps “OK” on the confirmation screen. The words “Reset App Data” are then greyed out.

Remove All Devices from MACO Profile

The member may have several devices enrolled with the same user profile. (See page 24 for information on how DAON handles situation where the member with a MACO profile attempts to enroll in MACO on a second device.)

This member may elect to remove all their devices from their MACO profile (saved on the DAON server). Once this is complete, the member must enroll in MACO again to use it to authenticate.

Step-by-Step Directions



12:00 PM

Settings & Info

Success CU Mobile
Version 3.2.01
Equal Housing Lender / Equal Housing Opportunity
Your saving federally insured to at least $250,000 and backed by the full faith and credit of the United States Government.

Authentication Options

Authentication FAQ

Reset App Data

View New Features Intro

12:00 PM

Back Authentication Options

The authentication options below are for your convenience and can only be configured to one account per device(s). However, this will not prevent logging into another account with the normal username, password and security question process.

Face Authentication

Pin Authentication

Voice Authentication

The above settings will apply to any registered device.

Fingerprint Authentication

Fingerprint settings will only apply to this device.

Quick Authentication

With this setting enabled, your last used authentication method will automatically prompt when needed. When this setting is disabled, you can change the authentication method each time you log in.

Reset Authentication Options on All Devices

option is for when you want to remove all device enrollments associated from this account.

Are You Sure?

Resetting authentication options on all devices will remove any Face, Fingerprint, Pin and Voice enrollments on all devices associated with your account.

Since you can enroll multiple devices using the same account, this option is for when you want to remove all device enrollments associated from this account.

To deactivate MACO on all devices, the member taps “Authentication Options” on the Settings & Info screen. Then the member taps “Reset Authentication Options on All Devices.”

When the member clicks “OK” on the confirmation screen, all devices attached to the profile are deactivated and removed from the profile on the DAON server. The words “Reset Authentication on All Devices” is then greyed out (not shown).

MEMBER-FACING QUESTIONS

Following are samples of the questions and answers the member sees in the “Authentication Questions” section of the App, accessed via Settings & Info. This list may have been altered and added to since this section of the booklet was last updated.

General

Which devices support biometric authentication? What else is required?

You will need iOs 9.0 or later for iPhone and 4.4 or later for Android. To utilize fingerprint, your mobile device will also need to have the capability for fingerprint scan.

How do I set up biometrics?

To set up biometrics for authentication, click on the ‘Locked’ icon in the Menu bar at the bottom. Then swipe to the left or right to see biometric authentication options. Once you select to enroll with one of the biometric options, you will enter your online banking credentials.

What if I am locked out from using my online banking username, password, and security question answer?

If you are locked out from standard login (using your username, password and security question), contact the credit union and have them reset your online banking credentials.

Do I need to enable location services?

No. You do not need to enable location services to use the biometric authentication methods.

What if I get a new phone, or want to add an additional device?

In Settings & Info select “Reset App Data.” This will clear the app data stored on your device but will not alter or delete your profile. You can also login on your new device where it will let you know a previous enrollment has been found and you can click "ok" to copy authentication enrollments.

What if I want to deactivate an authentication option?

In Settings & Info, use “Authentication Options" where you can turn each authentication type on/off. To use this authentication option again, you will need to re-enroll. From this same area, use “Reset Authentication Options on All Devices. This will completely erase your profile on any registered device. To use any authentication option later, you will need to re-enroll.

Can I login with my username, password, and security question?

Yes. You can swipe to where the username and password screen shows to login with your username, password, and security question.

Can more than one membership enroll for biometric authentication on my mobile device?

No. Only one membership is allowed per mobile device.

Do I have to click to authenticate each time?

You can choose to skip the step where you click the "authenticate with" button and instead automatically advance to signing in. To activate Quick Authentication, choose "Authentication Options" on the Settings & Info screen, from there you can select "Quick Authentication".

Can I lock myself out?

If you are using biometric authentication, after several failed attempts you will be temporarily locked out. You can still login with your username, password, and security question.

Also, if you fail to authenticate correctly several times, you may also be asked to enter your device passcode.

Voice:

What is required to enroll for voice recognition?

During enrollment you will say a passphrase that is presented on the mobile device. Three acceptable recordings are captured to create a voice profile.

Will voice enrollment allow for personal phrases to be recorded?

No. Personalized phrases are not supported.

Will voice recognition ask for access to the device microphone?

Yes. When enrolling for voice recognition the mobile app will ask for access to the device microphone.

PIN:

What is required to enroll for PIN?

During enrollment you will be presented with a number pad you will enter a four-digit PIN and then enter it again to confirm the number.

How do I authenticate with PIN?

You will select "Authenticate with PIN", where the number pad will be brought up on your device and you will enter the 4-digit PIN.

Will the PIN match the same PIN to my mobile device?

You have the ability to set the PIN to access mobile banking something different than your mobile device, or you can have these set to match.

Fingerprint:

Why am I not seeing the fingerprint verification?

Fingerprint authentication will only show on devices that support it. To use fingerprint authentication, there must be a fingerprint sample saved on the mobile device.

What is required to enroll for fingerprint?

During fingerprint enrollment, the sensor on the device captures a fingerprint sample that is compared with the fingerprint on the device.

Face:

Is Apple's Face ID supported?

Yes. If you have Face ID configured on your iPhone X, you will be able to enroll.

How do I take the picture required by face authentication?

The phone will give you a sliding rule at the top of the screen to indicate the quality of your face image. When the phone says “Blink” at the top of the screen, blink one time to activate the face recognition to take a picture.

What are some tips for enrolling in Facial Recognition?

- Center your face in the oval for best results.
- The quality meter above is a combination of several variables including device orientation, lighting, exposure and sharpness.
- When image qualify thresholds are met, the quality meter will be highlighted and must remain so for 5 seconds.
- Removing glasses is highly recommended as they may produce glare that can inhibit quality during enrollment.
- Certain types of hats or headwear can inhibit quality during enrollment.
- Excessive glare on the front or top of the head can inhibit quality during enrollment.

What is required to enroll for face recognition?

Face recognition uses your devices camera to capture images you will need to blink, nod, or shake. You will see messaging at the top of the device that helps you position the camera to capture a successful photo. The quality meter at the top of the screen will change color to indicate the quality of the image.

How do I change the Face Recognition Action?

The default for face recognition is for the member to blink to capture the image (this provides a liveness test). Other liveness options include shaking your head, or a nod. This can be changed from the Settings & Info, choosing Authentication Options, and then Face Authentication.

How do I need to hold my device when enrolling?

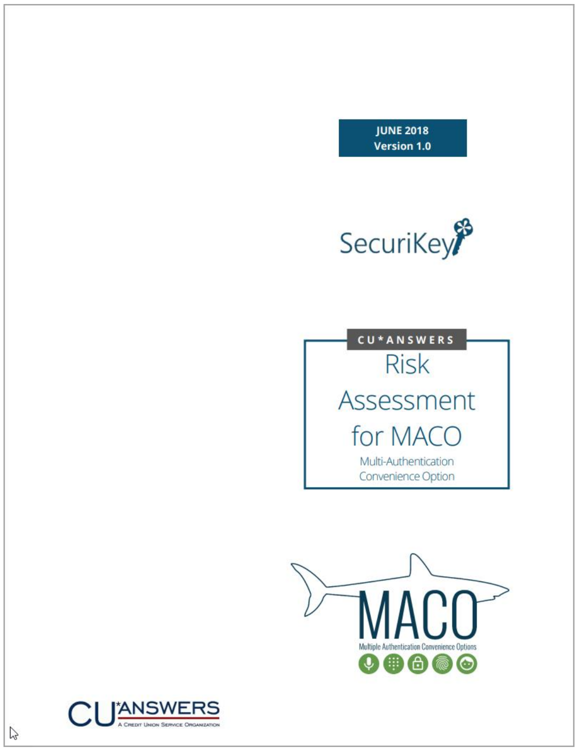
When enrolling for face recognition you will need to hold the device vertically, the messaging will change to "Hold Device Upright”.

When the camera is ready to take pictures, you will be prompted to "Hold Steady."

RISK ASSESSMENT: SECURIKEY QUICK REFERENCE GUIDE

CU*Answers offers the SecuriKey documents to give you quick access to the answers you need for your due diligence requirements. Find the SecuriKey Risk Assessment for MACO on the CU*Answers Risk Assessment Center page: https://www.cuanswers.com/resources/risk-assessment-center/. (Look for the SecuriKey logo.)

The Quick Reference Guide gives an overview of the important features of the product, and how to access additional information and services relating to the product. This is an excellent document to provide to examiners.



JUNE 2018
Version 1.0

SecuriKey

CU*ANSWERS
Risk Assessment for MACO
Multi-Authentication Convenience Option

MACO
Multiple Authentication Convenience Options

CU*ANSWERS
A Credit Union Service Organization

APPENDIX

- MACO EULA (Use Agreement)

TABLE OF CONTENTS

DAON LICENSING AGREEMENT

[CREDIT UNION]

Effective Date: [DATE]

These user terms of service, which include the Privacy Notice set out below in Part B (the “User Terms), govern your access and use of IdentityX Software (the "Services"). The Services are offered to you conditioned upon your acceptance of these User Terms. You agree that the User Terms constitute an agreement between CU*Answers ("Company", "us", or "we") and you or the entity you represent ("you" or "your"), and the User Terms will take effect when you use any of our Services or click an "I Accept" button or check box presented to you with these User Terms ("Your Effective Date"). You represent to us that you are lawfully able to enter into the User Terms, and, if you are entering into these User Terms for an entity, you represent to us that you have legal authority to bind that entity.

BY AGREEING TO THESE TERMS, YOU AGREE TO ARBITRATE ANY DISPUTES BETWEEN YOU AND US, WAIVING YOUR RIGHT TO A JURY, AS SET FORTH IN PARAGRAPH 23(C) BELOW. YOU FURTHER AGREE THAT THESE USER TERMS ARE PRESENTED WITHOUT WARRANTY.

This is an agreement between you, the user of this Software and the Licensee. By clicking the "Accept" button and/or using the Software, you accept these User Terms.

You have enrolled to use the Services. The Services may be presented to you under a different brand identity (e.g., "MACO"). The Services utilize, and include, both the IdentityX software downloaded to mobile devices, including, without limitation, the IdentityX Authenticator App, and to the software resident on backend servers (collectively, the "Software"). This includes, without limitation, software, including the object code and/or source code, functionality, concept, processes, internal structure, design, external elements, user interface, technology and documentation.

In order to use the Software, you must download the IdentityX Authenticator App on your mobile device. Acceptance of the User Terms is a precondition to downloading the IdentityX Authenticator App and use of the Services.

1. MODIFICATION OF THE USER TERMS

These User Terms are subject to change at any time and in the Company's sole discretion. The new revised version of the User Terms will be posted on this page or otherwise provided with notice to you. The modified User Terms will become effective upon such posting or, if we notify you by email, then upon sending such email message. Your use of the Services after such changes are implemented constitutes your acknowledgement and acceptance of the changes, and your agreement to be bound by the modified User Terms. Please consult these User Terms regularly to monitor for modifications. The date of last modification appears at the top of these User Terms.

2. PRIVACY POLICY

You agree that the Privacy Notice (as may be updated from time to time) governs any collection, use, and disclosure of your personal information. We will not make any changes that reduce your rights under the Privacy Notice without your explicit consent.

3. LIMITATIONS OF BIOMETRIC AUTHENTICATION

While biometric authentication provides you with greater security, you acknowledge that no security safeguard is infallible or, by itself, constitutes a comprehensive security solution. Even though you may be using biometric authentication, there is still a chance that your account may experience a security incident or breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, your account information. Such an incident or breach could result in your biometric data being compromised (e.g., mimicking or copying your biometric data).

Biometric technology is probabilistic, meaning that false matches and false non-matches can occur. The occurrence of such false matches, false non-matches, or other such products of probabilistic reasoning do not constitute product defects or breaches of these User Terms.

4. YOUR REPRESENTATIONS

In addition to any other representations and warranties contained in these User Terms, you agree that you have the authority, under the laws of the jurisdiction in which you reside, to make the following representations:

- You are sixteen (16) years of age or older, or have obtained legal authorization from your parent or legal guardian;
- You agree to keep the information on your account up-to-date, accurate, and complete, and, unless explicitly permitted, you will only create one (1) account;
- You understand that any security measure is not 100% impenetrable, including biometric authentication;
- Any biometric data you provide to us or to any of our third-party service providers is either your biometric data or the biometric data of a person for whom you are the legal guardian of or have obtained legal authorization from;
- The information you provide to us and any of our third-party service providers is complete, accurate, and up-to-date;
- If you are not a United States ("U.S.") resident, you confirm that the access to or use of our Services is not a violation of any export or import ban, or similar restriction in the country in which you reside; and
- You waive your right to any commercial products or research that is developed by us and/or any of our third-party collaborators.

5. PROHIBITED USE

In addition to any other representations and warranties contained in these User Terms and as a condition of your use of our Services, you represent and warrant that you will not use the Software to:

- Monitor, gather or copy any user information, content or material on the Services, without our prior written permission, on a manual or automated basis, including, but not limited to, by using any robot, "bot," spider, crawler, spyware, scraper, harvesting bots, engine, device, software, extraction tool or any other automatic device, utility or manual process of any kind;
- Frame or utilize framing techniques to enclose any trademark or other proprietary information (including, without limitation, any images, text or page layout);
- Seek to attempt to exploit or harm minors in any way;
- Engage in any activity or conduct that is unlawful, offensive, obscene, threatening, harassing, abusive, misleading, malicious, discriminatory, or that violates the terms, conditions, or notices of these User Terms, or any right of any third party;
- Violates any applicable federal, state, local, or international law or regulation (including, without limitation, any laws regarding online conduct, acceptable content, or the export of data or software to and from the U.S. or other countries);
- Attempt to circumvent the security systems of the Services in a manner not foreseen, agreed or expected (for example, attempted spoofing and similar is expected, as is testing of the biometric security such as liveness);
- Solicit login information or access an account belonging to someone else without their prior authorization;
- Attempt to gain unauthorized access to, interfere with, damage, or disrupt any parts of the Services, materials, other accounts, computer systems or networks connected to any CU*Answers server;
- Attempt to use the Services for any purposes other than those intended by CU*Answers, as determined by CU*Answers in its sole discretion;
- Attempt to probe, scan, or test the vulnerability of any of CU*Answers' system or network in a manner not foreseen or expected (see examples set out directly above);
- Use fake biometrics (including, but not limited to, presentation of pictures in printed or screen display form, use of masks, etc.) unless explicit permission has been granted by CU*Answers;
- Upload or submit any data or information that contains viruses or any other computer code, corrupt files or programs designed to interrupt, destroy or limit the functionality or disrupt any software, hardware, telecommunications, networks, servers or other equipment;
- Access, tamper with, or use non-public areas of the Services, CU*Answers’ computer systems, or the technical delivery system of CU*Answers’ third-party service providers;

- Engage in any activity or conduct through or in connection with the Services that restricts, inhibits, or interferes with anyone's access to or use of the Services, the proper operation of the Services, or, as determined by us, would harm CU*Answers or users of CU*Answers' Services or expose them to liability;
- Transmit, or procure sending of, any advertising or promotional material, including any "junk mail," "chain letter," "spam," or any other similar solicitation;
- Impersonate or attempt to impersonate CU*Answers, a CU*Answers employee, another user, or any other person or entity, including, without limitation, by using email addresses or usernames associated with any of the foregoing; and,
- Otherwise attempt to interfere with the proper working of the Services.

6. INTERNATIONAL USERS

The software, technology, and other information made available through our Services are subject to United States export controls and, potentially, the export and import laws of your jurisdiction.

No software, technology or other information from our Services may be downloaded or otherwise exported or re-exported to any person or entity on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders, or as otherwise prohibited by United States export control laws. You represent and warrant that you are not on any such list or located in, under the control of, or a national or resident of any such country.

Where legally permissible, CU*Answers may store, use, transfer, and otherwise process your personal information in countries outside of the country of your residence, which may have different data protection rules. CU*Answers will not transfer personal information outside the EEA to a third country or international organization that does not provide an adequate level of data protection, without your explicit consent.

7. MONITORING & REPORTING MISCONDUCT

CU*Answers shall have the right to monitor use of the Services to determine compliance with these User Terms. In the event of a violation of the User Terms, CU*Answers, at its sole discretion and without notice, has the right to suspend or terminate part of or the entirety of your account on a temporary or permanent basis.

If you have any knowledge of or suspicions that an individual is acting or has acted inappropriately or in violation of our User Terms, you should report your suspicions to CU*Answers by contacting us at irsc@cuanswers.com. If the misconduct is against the law or may be violating the law, you should report the person to the appropriate authorities, and only then to CU*Answers. You understand and agree that reporting any misconduct to CU*Answers does not obligate CU*Answers to take any action beyond what is required by law or cause to incur any liability to you or others.

8. CHANGES TO SERVICES

CU*Answers, at its sole discretion and without notice, reserves the right to amend or withdraw the Services at any time, including any services or materials provided on or through the Services, on a temporary or permanent basis. CU*Answers and its third-party service providers may charge a fee for any different or additional products, features, or services not included in your initial purchase. Your initial use does not entitle you to any different or additional products, features, or services that CU*Answers may offer. You acknowledge and agree that we are not liable if for any reason any part of our Services is unavailable at any time or for any period.

9. MOBILE BIOMETRICS APPLICATION LICENSE & RETENTION PERIOD

Typically, CU*Answers' demonstration applications, which are part of the Services, are provided at no cost for as long as you continue to use it. In accordance with our Privacy Notice, **we will retain your information for a period of six (6) months after the date of your last use of the demonstration application**, unless the applicable law requires a shorter retention period. In the event the applicable law requires destruction of your information at a certain time, we will comply with the applicable law.

10. INACCURACIES OR ERRORS

You assume all risks concerning the suitability and accuracy of the information within the Services. CU*Answers cannot guarantee that the descriptions, functionality, prices, availability, pictures, and other representations of the Services or Content are error-free, accurate, or up-to-date.

11. LIMITED LICENSE TO DISTRIBUTE CONTENT

All material included on or through the Services, and any other Services owned, operated, licensed, or controlled by CU*Answers, such as documentation, text, graphics, logos, images, photographs, audio clips, digital downloads, data compilations, and software (the "Content"), is the property of CU*Answers and/or its third-party licensors and is protected by United States and international intellectual property laws. Modification or use of the Content except as expressly provided in these User Terms violates CU*Answers 's intellectual property rights.

The Content may not be copied, distributed, republished, uploaded, posted, or transmitted in any way without the prior written consent of CU*Answers, except that:

> You may download, print, distribute, and use pages from the Services free of charge for your own informational, non-commercial purposes only;
>
> Any Content from the Services must not alter the original Services Content, including, but not limited to, the presentment of the Content;
>
> You may link to the services provided by third parties as long as the link does not falsely imply or suggest that CU*Answers has endorsed or is affiliated with the linked third parties; and
>
> You include or retain the following attribution on any materials you may distribute: CU*Answers. All Rights Reserved.
>
> The Content and Services may be updated or changed at any time without prior notice. In addition, if CU*Answers becomes aware that you are copying, modifying or distributing the Content or the Services other than for the permitted uses of the Services, CU*Answers reserves the right to revoke your right to these permitted uses.
>
> If you are unsure whether your use is permitted, please send a request with your proposed use to irsc@cuanswers.com so that we may evaluate your proposed use of CU*Answers' Services Content.

12. THIRD-PARTY PROPRIETARY INFORMATION CONSENT

If you wish to use material contained on the Services other than for your individual review and individual educational purposes, and the copyright ownership of such material is held by a third party, then you must secure the permission of such third party in order to use such material.

13. YOUR REPORTS AND FEEDBACK

Any of your feedback, comments, reports ("Reports"), or suggestions (collectively, "Feedback") directed at or provided to CU*Answers are the sole and exclusive property of CU*Answers, excluding your personal information as defined by the jurisdiction in which you reside.

After accessing or using certain Services, CU*Answers may request that you provide a Report describing any findings and issues encountered during your access or use of the Services.

You hereby irrevocably assign to CU*Answers any and all of your rights, title, and interest in any and all Feedback, including without limitation all worldwide patent, copyright, trade secret, moral and other proprietary or intellectual property rights therein, and waive any moral rights you may have in such Feedback. Upon our request and expense, you agree to execute documents and take further actions as CU*Answers may reasonably request to assist CU*Answers in acquiring, perfecting, and maintaining its intellectual property rights and other legal protections in the Feedback.

14. SECURITY

CU*Answers has implemented physical, technical, and administrative safeguards against unauthorized disclosure or access to your personal information. However, you agree that security safeguards, by their nature, are capable of circumvention and CU*Answers does not and cannot guarantee that personal information about you will not be accessed by unauthorized persons capable of overcoming such safeguards.

You are solely responsible for the activities under your account and for keeping any password (if applicable) confidential. Please notify us immediately at irsc@cuanswers.comif you believe there has been unauthorized access or activity under your account, or if your account information is lost or stolen. You cannot and will not hold CU*Answers liable for any loss or damage arising out of your failure to comply with these User Terms.

You cannot and will not hold CU*Answers liable for any loss or damage arising out of your failure to comply with these User Terms.

15. COMMUNICATIONS

In order to provide our Services to you, we may need to communicate with you. Typically, our communications are emails about Services-related matters. You agree that all agreements, notices, disclosures, and other communications that we provide to you electronically, via email or on the Services, satisfy any legal requirements. Where required by EU data protection law, we will request that you provide your consent in a separate form when we collect your personal information for communications.

16. INTELLECTUAL PROPERTY RIGHTS.

All data, including images, that you receive through the Services is proprietary information protected by trade dress, copyright, patent, trademark, and various other intellectual property rights and unfair competition laws, whether registered or not, unless noted, and may not be used except as provided in these User Terms or with the written permission of CU*Answers and its licensors. Any use of the Services or Content that is not expressly permitted by these User Terms will be considered a violation of the User Terms and may violate intellectual property laws.

CU*Answers and its licensors own all legal right, title, and interest in and to the Services and its entire contents, features, and functionality, including any intellectual property rights which subsist in the Services or content, whether those rights happen to be registered or not, and wherever in the world those rights may exist. Except as described in the Section entitled "Limited License to Distribute Content," or unless you have expressly agreed otherwise in writing with CU*Answers, nothing in the User Terms or the Services or any Content grants you or anyone a license to any CU*Answers trademark, copyrights or other intellectual property rights, whether by implication, estoppel or otherwise.

You agree you will not remove or obscure any proprietary rights notices (including copyright and trademark notices) that may be affixed to or contained within the Services. Further, you agree that you, or anyone else under your reasonable authority, will not copy, create a derivative work of, reverse engineer, modify, decompile, or otherwise attempt to extract the source code or other basis of CU*Answers, or its licensor's, technology. We reserve the right to immediately revoke your right to use our Services if you print, copy, download, modify, or otherwise use or provide any other person with access to any part of our Services in breach of the User Terms. In the event this happens, you will be required to return or destroy the materials in question.

17. THIRD PARTY TRADEMARKS

Trademarks displayed on the Services that are not owned by CU*Answers are the property of their respective owners, who may or may not be affiliated with CU*Answers. Nothing contained in the Services or Content should be construed as granting any license or right to use any third-party trademarks without the written permission of the third party that may own the trademarks. Your use of the trademarks, or any other Content on the Services, except as provided in these User Terms, is strictly prohibited.

18. WARRANTY.

All Services, including all software associated with the Services, is provided "as is" without any express or implied warranty of any kind. No liability is accepted by CU*Answers. Under no circumstances shall CU*Answers be liable for any special, consequential, direct or indirect loss or damage including without limitation, loss of profits, loss of data or loss of business opportunity.

19. LIABILITY.

IN NO EVENT WILL WE HAVE ANY LIABILITY TO YOU FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT YOU HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR MAXIMUM AGGREGATE LIABILITY TO YOU FOR ANY BREACH OF THE USER TERMS IS ONE HUNDRED US DOLLARS (USD $100) IN THE AGGREGATE. THE FOREGOING DISCLAIMERS WILL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW AND DO NOT LIMIT EITHER PARTY'S RIGHT TO SEEK AND OBTAIN EQUITABLE RELIEF.

You understand and agree that absent from your agreement to this limitation of liability, CU*Answers would not grant access to the Services.

20. THIRD PARTY PRODUCTS.

CU*Answers and its affiliates disclaim all liability with respect to third-party products that you use.

21. LINKED SITES.

Our Services or third parties may provide links to or be linked from other websites that are not maintained by or related to CU*Answers. CU*Answers does not endorse, and is not responsible for, the content of any such third-party websites or resources. You further acknowledge that CU*Answers will not be responsible or liable, directly or indirectly for any damages or loss caused or alleged to be caused by, or in connection with us of, or reliance on any such content, goods, or services available through any hyperlinked third-party website or resources.

22. TECHNICAL SUPPORT.

For information or technical support for the Services, please contact CU*Answers at irsc@cuanswers.com.

23. MISCELLANEOUS.

a. Entire Agreement. These User Terms and all documents incorporated into these User Terms by reference constitute the entire agreement between CU*Answers and you (including any prior versions of the User Terms) and supersedes any and all prior or contemporaneous communications and proposals, whether electronic, oral or written. However, certain provisions of these User Terms may be superseded by expressly designated legal notices or terms located on particular pages within our Services. You may also be subject to additional terms and conditions that may apply when you access or use the services, content or software of our affiliates, third parties, or collaborating parties.

b. -Dispute Resolution. The Parties may, with the assistance of the Centre for Effective Dispute Resolution (CEDR) seek to resolve the dispute by mediation. Each party shall bear its own costs and expenses incurred for mediation unless otherwise agreed; and any dispute, controversy, or claim arising out of, relating to, or involving these User Terms which the parties are unable to resolve through mediation within 30 days after the mediator has been appointed, or such other period agreed in writing, then the dispute will be referred and finally settled by arbitration.

c. -Arbitration. Any arbitration will be conducted on an individual, rather than a class-wide, basis. If you are located in, are based in, have offices in, or do business in a jurisdiction in which this section is enforceable, you agree that for any dispute, claim, demand, controversy, or cause of action arising under or in connection with the User Terms, including your use and access to the Services or any other content, shall be finally and exclusively resolved by binding and confidential arbitration under the American Arbitration Association's ("AAA") Commercial Arbitration Rules and Mediation Procedures and Consumer-Related Disputes Supplementary Procedures (unless where the applicable law such as Virginia law which provides for judicial review of arbitration proceedings). Where no claims or counterclaims exceed $10.000, the dispute will be resolved by the submission of documents without a hearing, unless a hearing is required by CU*Answers or deemed necessary by the arbitrator. It is your responsibility to pay any AAA filing, administrative, and arbitrator fees as set forth in the AAA Rules.

The parties further agree that the arbitrator shall have exclusive authority to resolve any dispute relating to the interpretations, applicability, enforceability, or formation of this agreement to arbitrate. Any such controversy or claim shall be arbitrated on an individual basis, unless both parties otherwise agree in writing. The arbitration shall be in English and held in Fairfax County, Virginia, U.S.A. The parties further agree to use their best efforts to conduct any dispute resolution procedures herein as efficiently and cost effectively as possible.

If you are not located in, and not based in, or not have offices in, and to not do business in the U.S., any arbitration between you and CU*Answers will be finally settled under the Rules of Arbitration of the International Chamber of Commerce ("ICC Rules") by one or more arbitrators appointed in accordance with the ICC Rules and will be administered by the International Court of Arbitration of the International Chamber of Commerce.

If, for any reason, a claim proceeds in court rather than arbitration, each party waives any right to a jury trial. You agree to the personal jurisdiction by and venue in the state and federal courts of Fairfax County in the State of Virginia or the United States District Court, Eastern District of Virginia located in Alexandria, and waive any objection to such jurisdiction and venue.

Any claim under these User Terms must be brought within one (1) year after the cause of action arises, or such claim or cause of action is barred.

This arbitration agreement will survive the termination of your relationship with CU*Answers.

d. Injunctive and Equitable Relief. CU*Answers retains the right to seek injunctive relief or other equitable relief in a court of competent jurisdiction to prevent the actual or threatened infringement, misappropriation, or violation of its copyrights, trade dress, trademarks, trade secrets, patents, or other intellectual property rights.
e. Headings. This section titles in the User Terms are for your convenience only and have no legal or contractual effect.
f. Assignment. You may not assign or delegate any rights or obligations under the Terms, and any such attempts will be deemed ineffective, CU*Answers freely assign or delegate all rights and obligations under the User Terms in part or in its entirety without notice to you.
g. Waiver. A failure by CU*Answers to exercise or enforce any right or provision of the Terms shall not constitute a present or future waiver of such right or provision. All waivers by CU*Answers must be in writing to be effective.
h. Severability. If any provision of the User Terms is found by a court of competent jurisdiction to be unlawful, void, or for any reason unenforceable, then that provision shall be deemed to severable from these User Terms and shall not affect the validity and enforceability of any of the remaining provisions. The remaining provisions of the User Terms shall remain in full force and effect. To the extent possible, any invalid or unenforceable portions will be interpreted to the effect and intent of the original portion.

24. NOTICES.

We may provide notice to you based on the contact information we have on file. To ensure that you receive our notices, please keep your contact information confidential and up to date.

CU*Answers may also provide a notice of changes to the User Terms or other policies by displaying a notice or link to the notice(s) on the Services. or electronic means, and shall be effective when received, with evidence of receipt.

25. LAW AND JURISIDICTION.

The construction, validity and performance of this Agreement is governed by the laws of the Commonwealth of Michigan.

PART B

PRIVACY NOTICE

1. ABOUT CU*ANSWERS AND THIS NOTICE.

CU*Answers is a cooperative credit union service organization providing software and services to credit unions. All equity in CU*Answers is held by credit unions exclusively, and there is no other private equity in the company. CU*Answers partners with companies like third party service providers ("Licensors") to provide software and services to credit unions for credit unions to serve their members better. CU*Answers also partners with other credit union service organizations to provide such third party service provider software and services to credit unions and their members.

This Privacy Notice (the "Notice") is intended to help you understand what information we collect and why we collect it, the specific purpose for using the data, and what happens to the data after it is used.

2. SCOPE OF THIS PRIVACY NOTICE.

This Notice applies only to the Personal Information collected by the IdentityX software ("the "Software"). This Software may be presented to you under a different brand identity (e.g., "MACO"). This Notice is provided by CU*Answers. We collect and process information about you as described in this Notice. We are committed to protecting the privacy of those with whom we interact. This Notice does not apply to any other interactions you have with CU*Answers or its partner credit union service organizations.

3. DATA SUBMISSION AND CONSENT.

IMPORTANT: BY USING THE SOFTWARE YOU ARE SUBMITTING PERSONAL INFORMATION TO US, AND YOU GIVE YOUR CONSENT THAT ALL INFORMATION THAT YOU SUBMIT MAY BE PROCESSED BY US IN THE MANNER AND FOR THE PURPOSES DESCRIBED IN THIS NOTICE.

4. DEFINITIONS.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Information. For purposes of this Notice, CU*Answers shall be deemed the Controller.

"Privacy Law" means all laws and regulations of the United States applicable to the Processing of Personal Information.

"Person" means an identified or identifiable natural person, who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Information" information that identifies, relates to, describes, or is reasonably capable of being associated with an identified or identifiable natural person under applicable Privacy Laws. Data that has been deidentified such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, with an identifiable individual is not "Personal Information."

"Data Breach" means a suspected or actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed.

"Processing" means any operation or set of operations that is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5. COLLECTION AND USE OF INFORMATION.

CU*Answers, and any credit union service organization partner using the Software does so for the purpose of verifying your identity, both initially and for subsequent verifications. Once the Software is initiated by you, the method of collection and the use of the data will be dependent on which verification method you use.

PIN. If you select and submit a PIN, that PIN is encrypted and sent via a secure Application Programming Interface ("API"). The PIN is stored securely on an IdentityX server at a CU*Answers location. The IdentityX application returns a response indicating verification success or failure.

VOICE. If you select voice verification, you will be prompted to record a passphrase using your device. This recording is encrypted and sent via a secure Application Programming Interface ("API"). When the recording reaches the IdentityX server at a CU*Answers location, an algorithmic data string is created from the recording. The data string is stored on the server in an encrypted format. The original voice recording is deleted once converted to the data string. The data string is akin to an asymmetric hash or encryption that stores passwords. Voices cannot be reverse engineered from the data string. The original voice recording is deleted once converted to the data string.

To authenticate using voice, you will speak the same passphrase, which will be sent via the secure API to the IdentityX server, converted and compared to the stored algorithmic data string. The IdentityX application returns a response indicating verification success or failure. The latest voice verification recording is deleted once compared to the original data string.

FACE (GOOGLE ANDROID ONLY). If you select face verification and your device uses a version of Google Android, you will use the application and your device's camera to capture a face image. This face image is encrypted and sent via a secure Application Programming Interface ("API"). When the face image reaches the IdentityX server at a CU*Answers location, an algorithmic data string is created from the face image. The data string is stored on the server in an encrypted format. The original face image is deleted once converted to the data string. The data string is akin to an asymmetric hash or encryption that stores passwords. Face images cannot be reverse engineered from the data string. The original face image is deleted from the IdentityX server within twenty-four (24) hours.

To authenticate using a face image, you will capture a face image, which will be sent via the secure API to the IdentityX server and compared to the stored algorithmic data string. The IdentityX application returns a response indicating verification success or failure.

FACE (APPLE iOS ONLY). If you select face verification and your device uses a version of Apple iOS, you will use the IdentityX application and your device's camera to capture a face image. The face image is verified through the Apple FaceID application and not IdentityX. Verification by the Apple FaceID application is converted to a token and sent via a secure API to the IdentityX server at a CU*Answers location. Based on the results of the Apple FaceID application, IdentityX returns a response indicating verification success or failure. Any verification information used by Apple FaceID is stored on the device you used for verification.

FINGERPRINT. If you select fingerprint verification, you will use your device's native fingerprint verification application to verify your identity. The fingerprint is verified by your device's native application and not IdentityX. Verification by the native application's fingerprint software is converted to a token and sent via a secure API to the IdentityX server at a CU*Answers location. Based on the results of the fingerprint application, IdentityX returns a response indicating verification success or failure. Any verification information used by the native fingerprint software is stored on the device you used for verification. Both Google Android and Apple iOS require that the user has already set up a fingerprint before it becomes an option for the member within our mobile app.

OTHER INFORMATION. The verification process requires we collect information to identify you and your device. Device information we collect may include, but not be limited to, your IP address and unique device identification information (e.g., your device ID, device type, RAM information, CPU information, and your device's operating system).

CU*Answers has specific measures in place in relation to any biometric data process, these measures relate to any biometric data, including its retention and destruction as may be required under applicable law. As used in this Policy, "biometric data" includes "biometric identifiers" and "biometric information". "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. "Biometric data" also includes any similar definitions under applicable law related to any biological characteristics of a person, or information based upon such a characteristic.

CU*Answers shall not capture your biometric data without asking for your explicit consent in advance. If you decide to share your biometric data, or a document which contains your biometric data, e.g., a passport or government issued identity document, CU*Answers shall process your biometric data solely to perform the specific services you have requested and to improve the performance and/or accuracy of such services. Neither CU*Answers nor its affiliates or sub processors will sell, lease or trade any biometric data that it receives from you through your use of CU*Answers' Services.

CU*Answers will only retain biometric data for the relevant retention period specified in Records Retention and Protection Policy. Specifically, when the purpose for collecting biometric data has been satisfied, CU*Answers shall permanently delete such biometric data, and in any case any biometric data collected from you by CU*Answers shall be automatically deleted within 6 months of your last interaction with the CU*Answers website.

6. LEGAL BASIS

The legal basis for the processing of your Personal Information is one of the following:

a) Consent; or

b) Notice; or

c) To provide the Service for which you entered into a contract with us when you accepted the User Terms when you accessed our Services or used our website and downloaded the Application to use the Services; or

d) To comply with a legal obligation to which we are subject.

Please note that the provision of Personal Information is a requirement of the contract and is necessary to enable us to provide the Services to you through the Application. Where you have provided your consent for us to process your Personal Information, you have the right to withdraw your consent for all our portions of the processing of your Personal Information at any time.

7. CONTROLLER OBLIGATIONS.

CU*Answers has implemented commercially reasonable technical and organizational security measures designed to protect Personal Information against loss, misuse, and unauthorized access, alteration, disclosure, or destruction. We also have implemented measures to maintain the ongoing confidentiality, integrity and availability of the systems and services that process Personal Information and will restore the availability and access to data in a timely manner in the event of a physical or technical incident. CU*Answers will comply with all applicable privacy and data protection laws. Where it is required by law to disclose Personal Information, CU*Answers may disclose Personal Information only to the minimum extent necessary to comply with such law.

Although CU*Answers has implemented commercially reasonable security, CU*Answers cannot guarantee your information will never be disclosed in a manner inconsistent with this Notice. If a breach of your Personal Information were to occur, we will work with your credit union to notify you, as required by applicable law.

CU*Answers expects you to be responsible for the security of your Personal Information by taking precautionary measures, such as keeping any account password/PIN (if applicable) confidential and using secure wireless connections. In addition, the Software should not be used on a device shared with other persons.

8. RETENTION.

CU*Answers will retain your Personal Information for no longer than is necessary to enable you to use the Software, and to comply with our legal obligations, resolve disputes, enforce our agreements and for other business reasons permitted by applicable laws and regulations. CU*Answers will take steps to dispose of your Personal Information securely and permanently, according to applicable laws and regulations, once your Personal Information is no longer needed for any of the foregoing reasons.

Even if we delete your information from active databases, the information may remain on backup or storage media to the extent allowed by applicable data protection laws and regulations.

9. CHILDREN’S PRIVACY.

Due to federal law (as reflected in the Children's Online Privacy Protection Act), YOU MUST BE AT LEAST 13 YEARS OLD TO USE THE IDENTITYX SOFTWARE. IF YOU ARE BETWEEN 13 AND THE APPLICABLE AGE OF MAJORITY, PLEASE REVIEW THIS AGREEMENT WITH YOUR PARENT OR GUARDIAN.

CU*Answers does not knowingly solicit or collect Personal Information online from children under the age of 13 without prior verifiable parental consent. If we learn that a child under the age of 13 has submitted personally identifiable information online without parental consent, CU*Answers will take all reasonable measures to delete such information from its databases and to not use such information for any purpose (except where necessary to protect the safety of the child or others as required or allowed by law). If you become aware of any Personal Information we have collected from children under 13, please email us at irsc@cuanswers.com.

Minors under 18 years of age may have Personal Information that they provide to us deleted by sending an email to irsc@cuanswers.com requesting deletion. Please note that, while we make reasonable efforts to comply with such requests, deletion of your Personal Information does not ensure complete and comprehensive removal of that data from all systems.

10. CONTACT US.

If you have any questions about this Notice, our data handling practices, or the IdentityX Software, you can contact us at:

EMAIL: irsc@cuanswers.com

U.S. MAIL: 6000 28th Street SE, Grand Rapids, MI 49546.

This document is current as of December 2023.