velera

USER GUIDE

IDCheck Setup and User Guide

3/10/2025

Velera LEGAL DISCLAIMER

The attached material and any subsequent discussion with Velera representatives are not intended to be, and shall not be construed as legal advice, does not create any attorney-client relationship, nor is it a comprehensive list of issues that could impact your business and its compliance with applicable legal requirements. Because of the generality of this communication, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice from your counsel based on the facts and circumstances of your particular situation. Further, Velera does not, by agreeing to process the settings you request in connection with your review of these materials, warrant or guarantee the effectiveness, accuracy, or completeness of your settings, or the compliance of your settings with applicable requirements.

Contents

Introduction 5
Purpose of This Guide 5
How to Use This Guide 5
Shared Branch 5
IDCheck Shared Branch 6
Successful Launch 6
Communications 6
Marketing for Members 7
Training Your Staff 8
A Launch Checklist for Shared Branch 9
Member Experience 10
Visiting Member Experience Overview 10
Instructions for Visiting Members 11
IDCheck Shared Branch Administrators 17
Set Up and Maintain Users 17
Fill in All Required Fields 17
Enable the IDCheck Tile 18
Frontline Staff 19
Provide Assistance to Members 19
Access the IDCheck App 19
Authenticate a Member 19
Details on the Verify Information Screen 23
Troubleshooting and Error Messages 24
Shared Branch Credit Unions 24
Reports 26
Daily Operational Reports 26
Dashboard 26
Shared Branch FAQ 27
Contact Information 31

System Disclaimer: IDCheck regularly updates its user interface. The most recent changes may not be reflected in the screenshots or functionality, but the principles in this document remain the same.

Introduction

Purpose of This Guide

- This guide provides information about IDCheck Shared Branch, which is used when a Shared Branch member goes to a Shared Branch location to perform a transaction using the IDCheck Shared Branch QR code to authenticate.

  There are also IDCheck OTP products used in the Contact Center environment, but they are not included in this guide.

How to Use This Guide

Shared Branch

This guide can be used by your credit union for the following:

- **Visiting members** – Members who belong to another credit union and visit your credit union to conduct transactions. Information in this guide can assist as you:
  - Plan and prepare communications with members.
  - Train your staff about the member experience.
- **Admin staff at your credit union** – People who set up IDCheck for current staff and who perform maintenance. They will:
  - Set up new user and admin accounts for activation of IDCheck at your credit union.
  - Test access for admins and users.
  - Set up and test accounts in an ongoing manner as new employees are hired and others need access to IDCheck.
- **Frontline staff at your credit union** – Staff who use IDCheck to:
  - Assist visiting members as needed.
  - Complete the authentication process that members begin.
  - Determine if transactions should be completed, and then:
    - Perform transactions for visiting members, or
    - Follow procedures to help avoid the risk of fraud.
- **Management or senior staff** – Access to reports will be available in the Insights Center for:
  - Staff who view reports to analyze data and make decisions based on that data.

IDCheck Shared Branch

Successful Launch

To help ensure a successful rollout of IDCheck and a positive experience for visiting Shared Branch members, consider the factors described in this section as you plan your communications, marketing, and training.

Communications

For Your Members

- **Educate members on the authentication process using IDCheck.**

  A targeted approach is recommended, focusing on only the members who use Shared Branching. To find out which members visit Shared Branch locations, you can use the Insights Center or information from your core data processor. Focusing on those members will help save time for members, who will understand the process and know what has changed since their last visit.

For Your Staff

- **IDCheck administrators need to know:**
  - **How to set up your credit union to use IDCheck.**

    Important!

    Your frontline employees will need to use My Co-op to access IDCheck. My Co-op is the single launching point for the IDCheck tile.

    For support with ensuring your users can access IDCheck via My Co-op: Details on creating My Co-op users and changing user attributes for existing My Co-op users are in the My Co-op Delegated Admin Console Guide and the "My Co-op Administrator" eLearning course in the Learning Portal. You can also contact your Client Growth Executive or Client Service Delivery at 800-782-9042, option 3, or via clientcare@coop.org.

    For information about how to sign in to My Co-op: See the My Co-op End-User Guide.

  - **How to perform an ongoing IDCheck admin role.**

    Admins will continue to set up access for new employees and others who need to use IDCheck.

- **Frontline staff need to know:**
  - **That they will perform a key role in the daily use of IDCheck.**

    The success of the member experience will rely on frontline staff's knowledge about using IDCheck, which saves time in the verification process.
  - **How to guide users who need assistance.**

    Frontline staff will need to be knowledgeable about the complete member experience so they can address any questions from visiting members and provide any needed assistance, guiding the visiting members through the authentication process.
  - **How to complete the verification process with IDCheck before conducting transactions for visiting members.**

    Frontline staff will use IDCheck and your business practices to determine whether to perform a requested transaction or not. IDCheck adds an additional layer of protection against fraud, and your frontline staff will play an important role in minimizing risk to your credit union.
  - **Good judgment and sound practical sense will play an important role.**

    Frontline staff will always need to use good judgment when conducting any Shared Branch transactions. If the person standing before the staff member is clearly not the member validated through IDCheck, the staff member should follow your credit union's standard process for escalation to a next-level manager or fraud resource officer.
- **Your branch manager needs to know:**
  - **IDCheck materials need to be readily available to visiting members.**

    For example, a table tent with a sign displaying the QR code that visiting members need to scan, and any other materials your credit union determines are helpful.
- **Management/senior staff who analyze data and make decisions based on that data need to know:**
  - **Reports are in the Insights Center.**

    When IDCheck is activated, reports will be available to designated staff in the Insights Center. They can view daily operational reports and a dashboard.

Marketing for Members

Marketing and education considerations for your members can include the following.

- **Market to your members before and during the implementation of IDCheck.**

  Education for members is important so they know what's new and what they can expect. Determine the best cadence for your marketing plan. Marketing materials can be found in the IDCheck Onboarding Guide and include a focus on the following:
  - Differences that members will experience when they first visit a Shared Branch that uses IDCheck.
  - Members can find out if a credit union they plan to visit uses IDCheck by contacting that credit union.

  - Members will see a sign in the credit union with the QR code to begin the authentication process.

- **Let members know there is new service for their protection.**

  Help users get ready for their next Shared Branch visit by letting them know IDCheck is a fraud-protection tool for them and for your credit union.

  - IDCheck is a secure and streamlined verification process that saves time when they visit a Shared Branch credit union.
  - The authentication process adds a layer of protection to help prevent fraud, so the credit union they visit knows the member is who they say they are.
  - Visiting members will want to bring a government-issued ID.

    Note IDCheck does not support military IDs due to a federal regulation that does not allow federal IDs to be copied/photographed.

- **Bring a current government ID.**

  Members will need a non-expired government ID, such as a driver's license, to conduct the transaction. They may also want to have their account number and last four digits of their Social Security number. This data is encrypted in the secure application.

Training Your Staff

Considerations when training your staff include:

- Frontline staff need to understand the complete authentication process with IDCheck, both from their perspective and the visiting member's. Staff needs to be knowledgeable so they can provide assistance as needed.
- Copying frontline staff on communications is a good way to keep them in the loop on communications with members. This may be a good practice to help inform staff.
- Learning Portal – "IDCheck by Co-op" is a video available for use when training your existing staff and onboarding new staff. This video demonstrates the member experience and frontline staff experience, and includes pictures of screens that members see on their smart device and staff see on their computers.
- Let your credit union's management know how to access reports via the Insights Center.

A Launch Checklist for Shared Branch

To help ensure a successful rollout of IDCheck at your credit union, you can use this checklist as a guide when preparing for your launch.

Marketing

_____ Members know what to bring when visiting a Co-op Shared Branch location.

_____ Members know what they are expected to do at a Shared Branch.

_____ If you make the QR code available for visiting members to pre-validate before arriving at your credit union, let members know how they can perform pre-validation.

Technical

_____ Credit union's IDCheck admin has completed the My Co-op setup.

_____ IDCheck tile is in My Co-op for staff to access.

_____ Access for each IDCheck admin and frontline staff has been set up and verified.

Business Procedures

_____ Your credit union has developed a plan of action in the case a visiting member's ID is not validated.

_____ Frontline staff knows how to manage situations where fraud is suspected.

Training and Communication

_____ Credit union staff all understand the expectations for their role.

_____ Depending on your credit union's escalation procedures, ensure the appropriate staff knows who to contact if any problems are experienced with IDCheck.

_____ Frontline staff has been trained on what they need to do and what visiting members need to do.

_____ Frontline staff is copied on emails to members concerning IDCheck.

_____ Management and senior staff know what reports IDCheck produces and how to access them in the Insights Center.

Branch

_____ QR code is displayed in your credit union for visiting members.

_____ Any additional member-facing information about IDCheck you want to provide for visiting members is in place.

Member Experience

When a visiting member arrives at a Shared Branch location, they follow the steps in this section to bring up IDCheck on their smart device and proceed through the validation process. Then they receive an access code, which they take to your frontline staff to perform their transaction.

> **Note** Credit unions can choose to make the QR code available for visiting members to pre-validate before arriving, such as on the credit union's homepage.

Visiting Member Experience Overview

IDCheck validates approved government-issued identification documents of members who visit a Co-op Shared Branch location.

When members visit your Shared Branch, they will use a smart device, such as their smartphone, to scan the QR displayed in the credit union. Then the app opens on their device, and they follow three basic steps that the IDCheck app guides them through.

The following table outlines visitor actions. Details are provided in the next section of this guide, Instructions for Visiting Members.

Step	Visitor Actions
How to begin	Scan the IDCheck QR code in the credit union.
1. Specify credit union.	Provide information about the member's home credit union. They can enter information in one, some, or all fields, or skip this step by tapping Skip Step near the bottom of the screen.
2. Enter information.	Provide their member account number and last 4 digits of their SSN.
3. Take picture of ID and a selfie.	Member takes picture of front and back of their government-issued ID, and then takes a selfie. *Socure is a partner that supports IDCheck. The selfie provides an additional layer of fraud protection because IDCheck compares it to the picture on the ID.*
4. Receive access code.	IDCheck validates the member and provides an access code. Member gives the code to frontline staff, who completes the authentication process and performs the transaction for the member.

Return Visitors and Devices

Return visitors will scan the QR code and be prompted to use the authenticated information that IDCheck recognizes. Then the member skips all the steps they needed to do the first time they used IDCheck, and the member receives an access code.

The authentication process associates the *device* to the authentication. In instances such as a returning visitor has a new device, new picture on ID, or new ID, the member must proceed through all the steps of the authentication process again.

Instructions for Visiting Members

The instructions on the following pages are for Co-op Shared Branch members who visit your credit union.

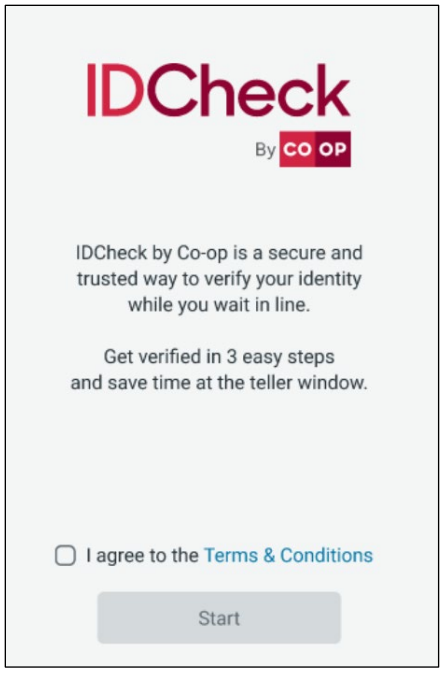
You can use these instructions when training your staff in the details of the member experience and when developing materials for members.

Use IDCheck When Visiting a Co-op Shared Branch Credit Union

Note If the Shared Branch you visit uses IDCheck for member verification, a prominently displayed sign with the QR code will be in the credit union.

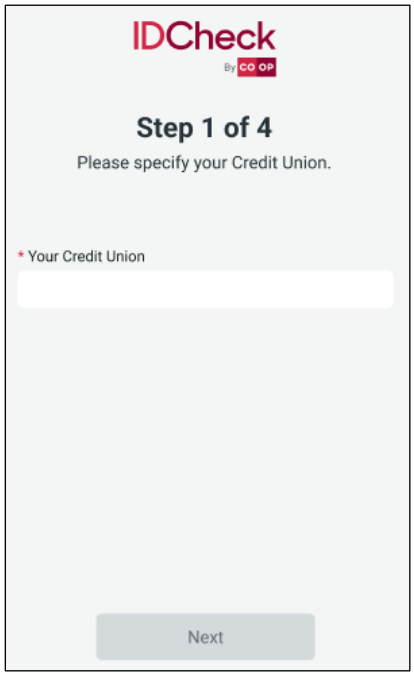
Scan the QR code displayed in the branch.

When visiting a Shared Branch that uses IDCheck, scan the QR code on your smart device, such as a smartphone, accept the Terms & Conditions, and tap **Start.**



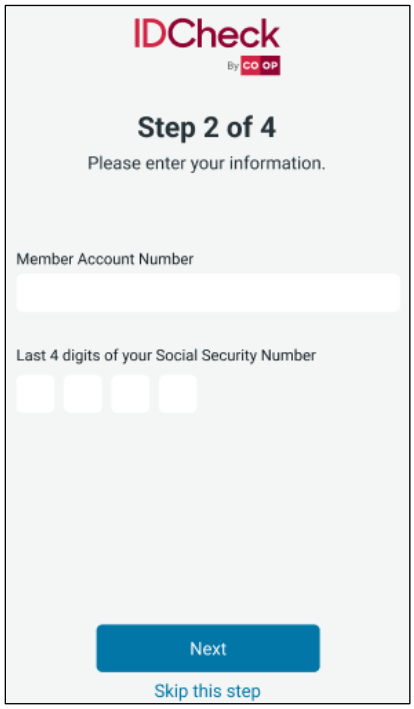
Provide your credit union's name.

Type the name of your home credit union, and tap **Next**.



Supply your information.

Type your account number and the last 4 digits of your SSN. Then tap **Next**.

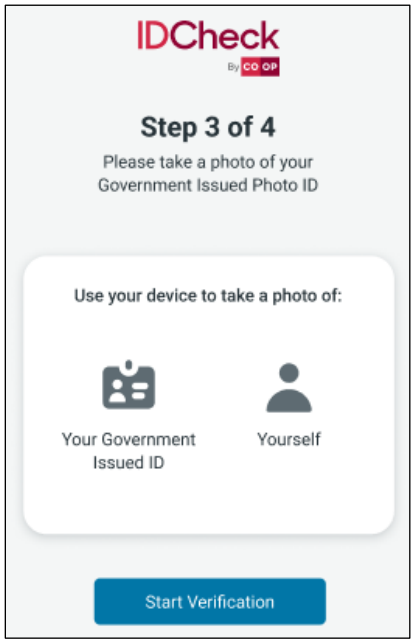


Take a picture of your ID.

Select **I Agree** to accept the Terms for Socure to authenticate.

> **Note** Socure is the partner supporting IDCheck.

Tap **Start Verification**.



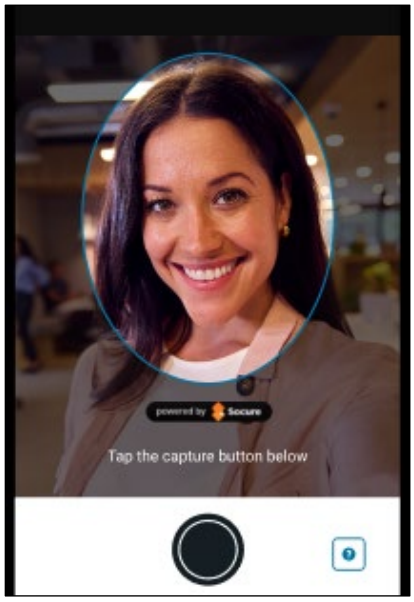
IDCheck guides you in taking a picture of the front and back of your government-issued ID.

When taking a picture of your ID:

- Be sure to allow access to your camera.
- A frame appears around your ID so you know how close to hold your device, such as a smartphone, to help ensure all parts of the ID are captured. Line the guide up with the shape of your license.
- Try a more plain (solid) background that contrasts with the ID (is a different color than the ID).
- Avoid glare and shadows.
- Hold the device steady.

Take a selfie.

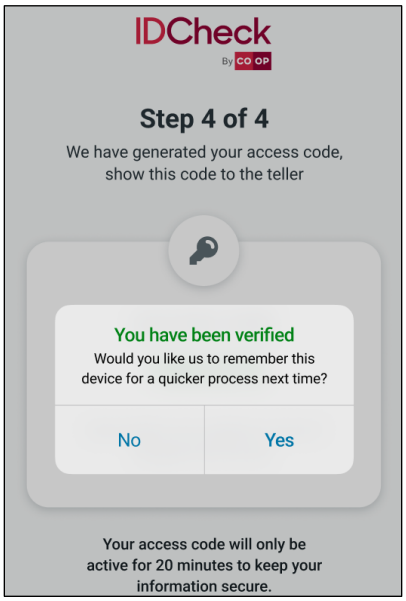
IDCheck guides you to take a selfie, which is used to validate your ID.

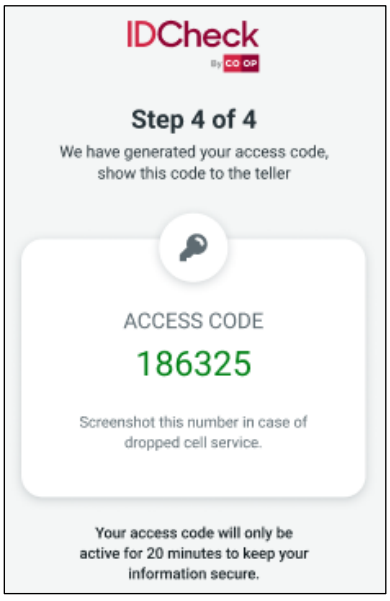


Receive an access code.

When verification is complete, you receive an access code. The code will let the credit union know your ID has been verified. Take the code to the credit union's frontline staff, who will perform your transaction.

- If this is your first time going through this process, you will see a pop-up on this screen offering the option to be remembered for an expedited flow the next time.





Note The access code is active for 20 minutes. If it expires, you need to begin the process again by scanning the QR code.

Stored verification option

On your next visit, IDCheck prompts you to use the authentication information it recognizes. You can skip the other steps (you do not need to take a photo of your ID or yourself) and then you will receive an access code to take to the frontline staff.

> **Note** On a subsequent visit, IDCheck will prompt you to provide information and take a picture of your ID and selfie again if a situation like the following has occurred: You have a new smart device, or the ID previously used for verification has expired.

IDCheck Shared Branch Administrators

This section addresses how staff in the IDCheck administrator role will set up new users and perform ongoing maintenance for IDCheck at Shared Branches.

Set Up and Maintain Users

- **Make sure your credit union is ready to turn on the service** – Ensure the IDCheck icon is available to your credit union via My Co-op.
- **Test that each admin and frontline user can access the IDCheck tile via My Co-op.**
- **Test reports** – Make sure the appropriate persons know they can access daily operational reports and dashboard in the Insights Center.
- **Set up new users and add users ongoing** – Assign IDCheck app permissions to frontline staff.

  Important! You will need to enter *all* required fields, including the Springboard Org ID (your financial institution's 4-digit client ID number provided by us). Be sure to have all this information before you begin. See Fill in All Required Fields in this guide.

- **Change info/anything about existing user accounts** – Change any information or user permissions. For example, staff changes role and needs access, or needs to have access removed.
- **If there are problems, contact your Client Growth Executive or Client Service Delivery.**

Fill in All Required Fields

Details on creating My Co-op users and changing user attributes for existing My Co-op users are in the My Co-op Delegated Admin Console Guide and the "My Co-op Administrator" eLearning course in the Learning Portal. You can also contact your Client Growth Executive or Client Service Delivery at 800-782-9042, option 3, or via clientcare@coop.org.

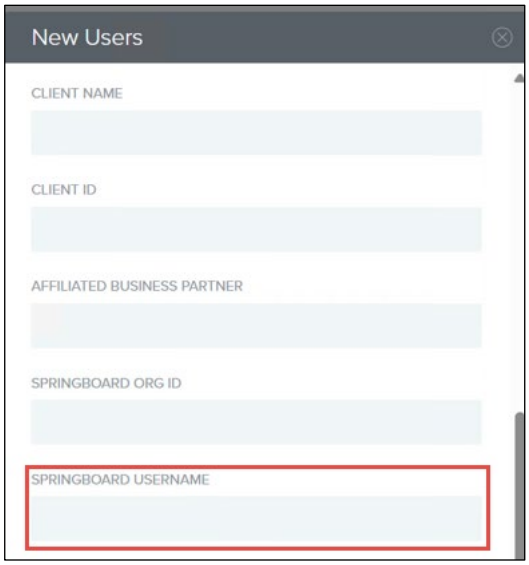
Important!

- Be sure to have all the information you will need to enter *before* you start to set up a new user or add IDCheck for an existing My Co-op user.
- All required fields must be entered before you select Save, including the **Springboard Org ID**, which is also known as your credit union's 4-digit Client ID number provided by us.

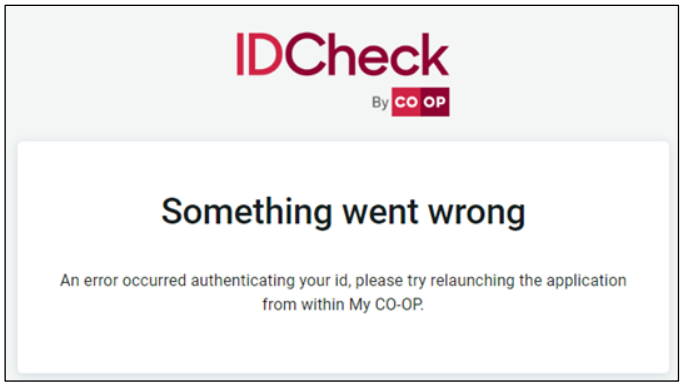
If the Springboard Org ID, which is your Client ID, is not entered before selecting Save – even if you plan to return to complete the setup later – the IDCheck tile will not work for the staff member whose account you are setting up.

Tip Your Springboard Org ID can be found on your bill, in the Insights Center reporting (which is filtered by the 4-digit company code), or you can ask your Client Growth Executive for this.

When creating My Co-op users or changing user attributes for existing My Co-op users, make sure you enter your Springboard Org ID, also known as your Client ID.



Or you may experience the following message:



Enable the IDCheck Tile

Users that need to use IDCheck will need the SharedBranching group membership assigned to them so that the IDCheck displays in My Co-op.

For details on assigning group memberships, see the My Co-op Delegated Admin Console Guide.

Frontline Staff

Provide Assistance to Members

As frontline staff for your credit union, you play an important role in not only completing the authentication process and performing transactions for visiting members, but providing any assistance they might need.

To learn about the visiting member experience, see the Member Experience section in this guide, especially the Instructions for Visiting Members.

Access the IDCheck App

Frontline staff accesses IDCheck via My Co-op. They can bring up the IDCheck app as they need it, or open it at the start of the day and keep it open throughout the day.

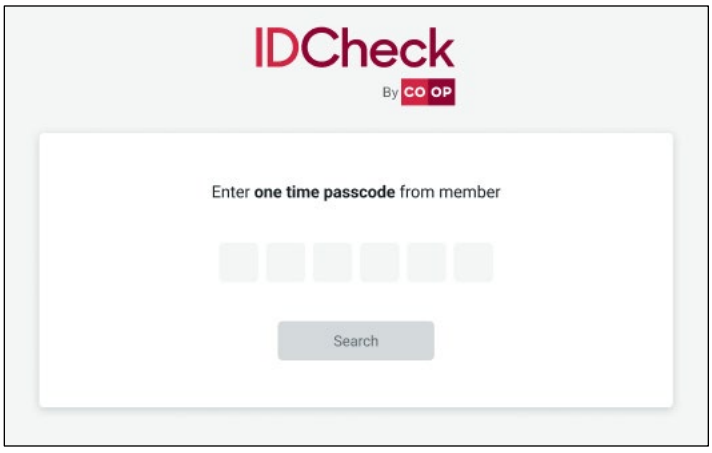
> **Note** If you have not used My Co-op before, you can refer to the My Co-op End-User Guide for directions on first-time use. My Co-op End-User Quick Reference Guide is also available, which contains high-level instructions for initial sign-on.

- In My Co-op, click on the **IDCheck app**.

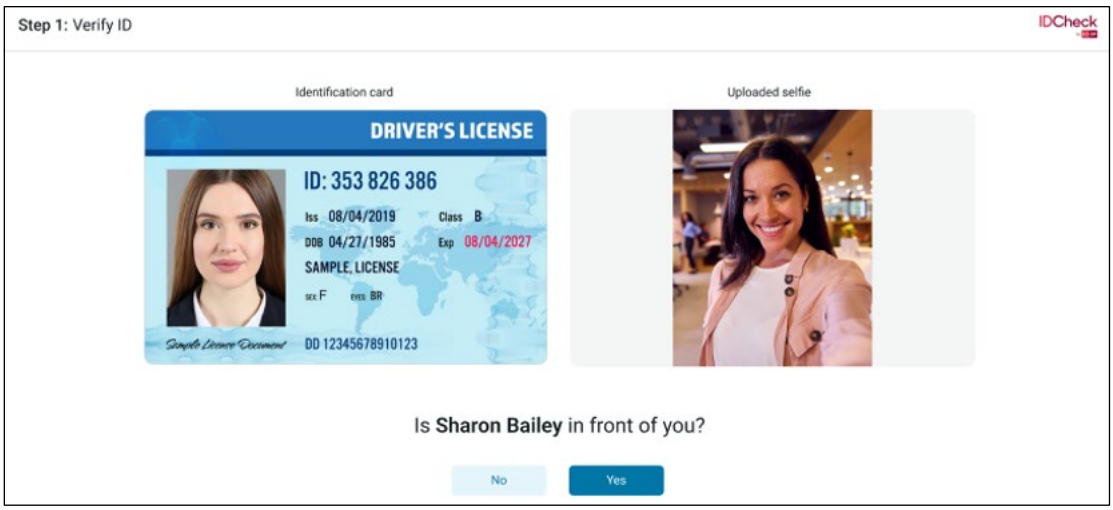
Authenticate a Member

In IDCheck, frontline staff performs the following steps to authenticate a member:

1. Enter the IDCheck access code that the visiting member provides, and click **Search**.



A screen appears with a picture of the ID that the member scanned.



2. Verify if the visiting member is in front of you (that they match the scanned ID), and select Yes or No.

   Note Frontline staff should always use good judgment when conducting shared branch transactions.

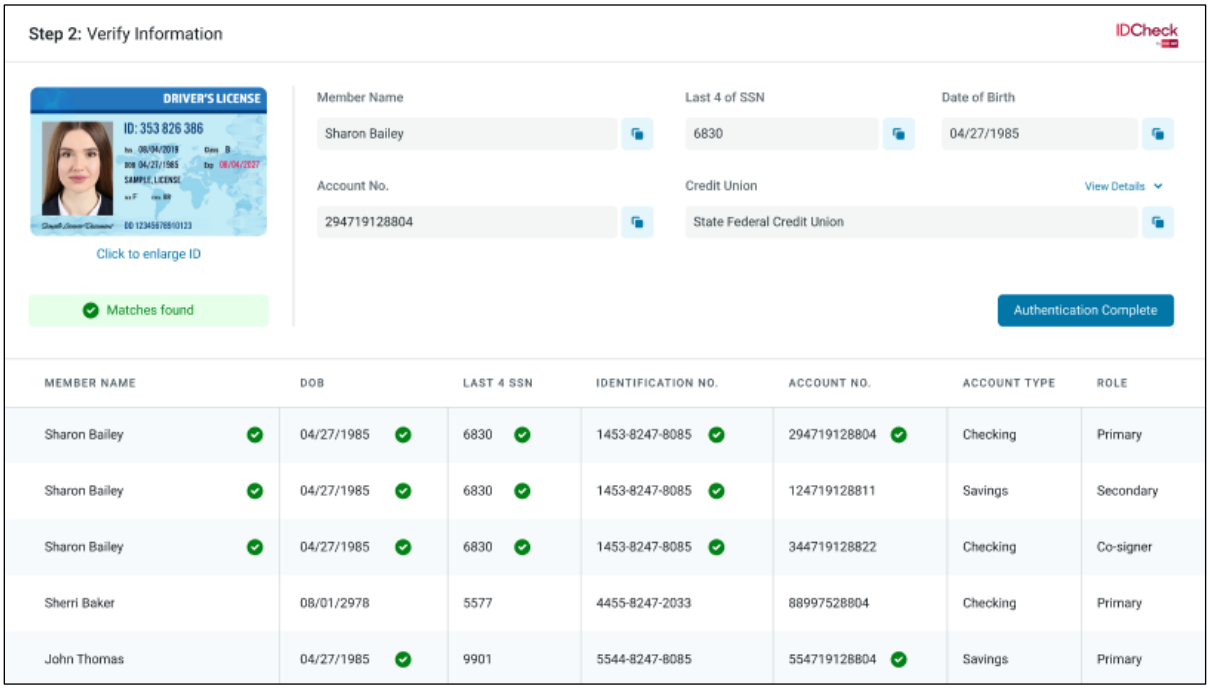
   - If **Yes**, continue with the transaction.

     When you reply Yes, a screen appears displaying the visiting member's information, which matches what the member entered and the information in your credit union's core database. Each line of the screen displays information about an account, as shown on the following page of this guide.

   - If **No**, follow your credit union's standard process for escalation to a next-level manager or fraud resource officer.

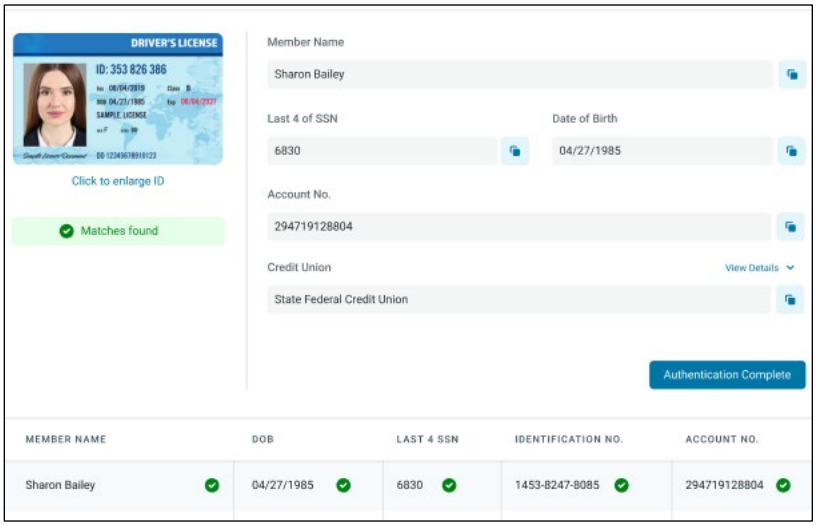
Example

The following screen shows that Sharon Bailey has two checking accounts and a savings account.



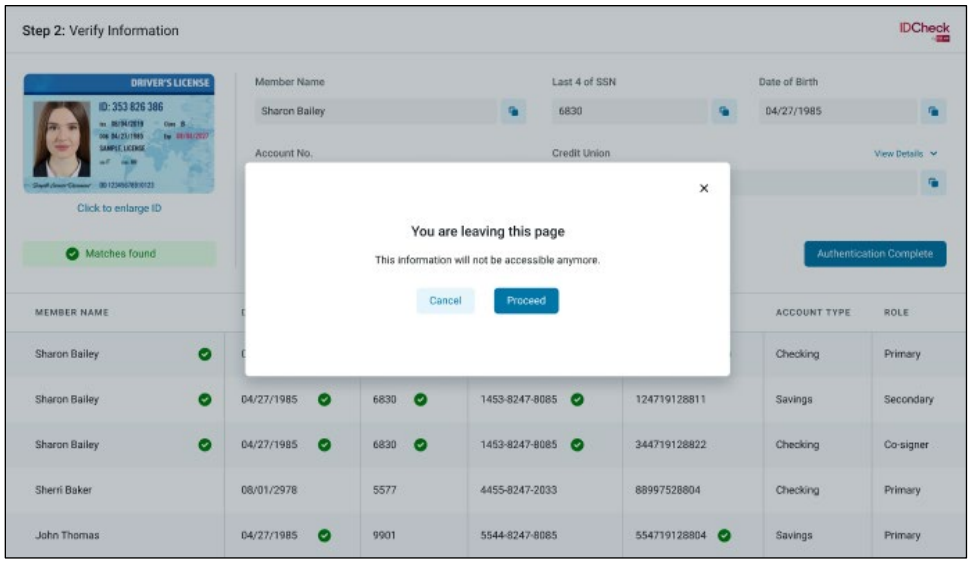
- **To copy account information (such as account number):** You can select the copy icon.

3. Perform the requested transaction for the visiting member.



4. After performing the transaction, you can leave the IDCheck screen open in case the member wants to perform another transaction or close the IDCheck session for this member.

   - **To leave the IDCheck screen open for this member:** Select **Authentication Complete**, and click **Continue**.



   - **To close the IDCheck session for this member:** Select **Authentication Complete**.
     - To go back to the IDCheck landing page, click **Proceed**.
     - To dismiss the prompt, click **Cancel**.

Details on the Verify Information Screen

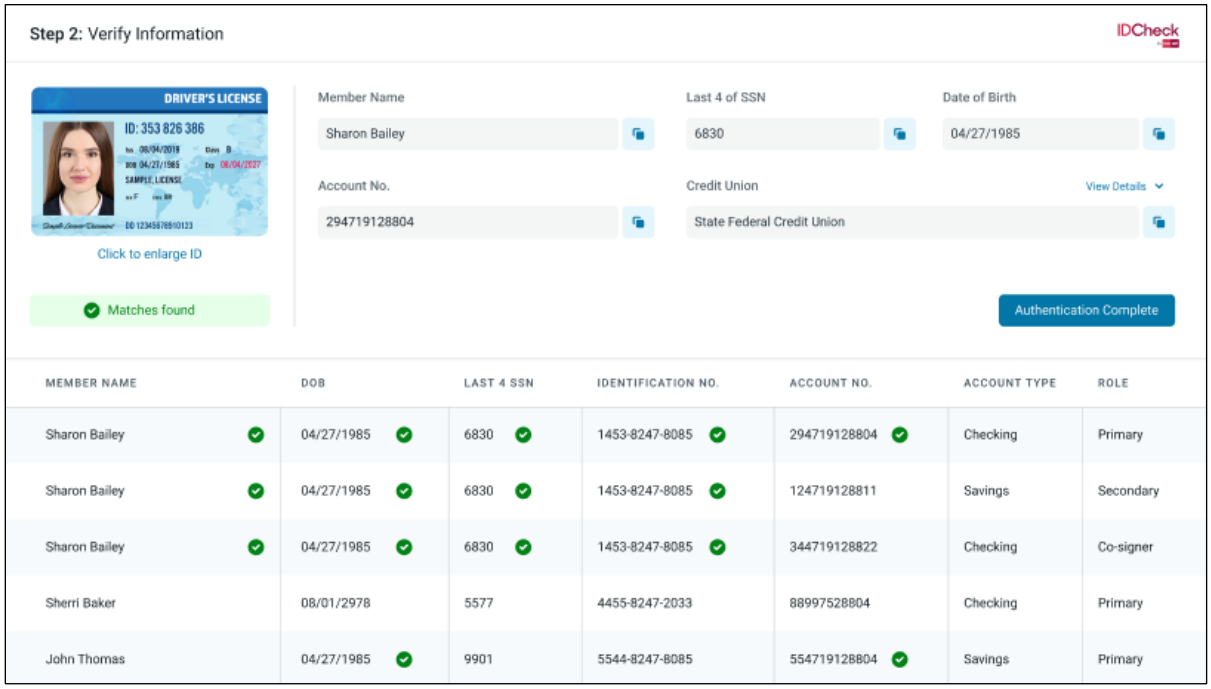
Information displayed:

- Member's Name
- DOB
- Last 4 SSN
- Identification No
- Account Number
- Account Type
- Role

Green circle with check mark – Information provided matches with your credit union's core.

If there is no green circle with check mark – Information does not match; needs additional verification according to your credit union's procedures. While the absence of a green circle with a check mark could indicate potential fraud, it could also indicate that a visiting member may have inadvertently entered incorrect information. If a green circle with a check mark is not present, proceed according to your credit union's processes and procedures.

Note Good judgment and sound practical sense will play an important role. When conducting a Shared Branch transaction, frontline staff always need to use good judgment. For example, if the person standing before them is clearly not the member validated through IDCheck, your credit union's process for such situations should be followed.



Note A green circle with a check mark does not appear if a person is not a member – such as a parent making a deposit to a child's account. The ID will be verified, but the data would not match. Good judgment and sound practical sense play an important role in the verification process.

Troubleshooting and Error Messages

Some error messages that may be experienced are listed in this section. Other errors could occur, in which case follow your established procedures for support, such as contacting your Client Growth Executive or Client Service Delivery.

Shared Branch Credit Unions

Visiting Members

Message	Description	What To Do
"ID was not recognized." "Failure to verify ID. Try again or see a teller." "Something went wrong, try again or see a teller". "Failed to obtain access code, try again or see a teller." "We could not generate an access code. Proceed to the teller."	Identification was not validated.	Visiting member needs to go to teller line.
"Could not find a matching account, check your details and try again."	Account not found during member verify call.	Member needs to call their home credit union.
Notification to retake the picture.	Member took blurry picture, so their ID could not be validated.	Work with the member to hold the smart device still and take a clearer picture.

Frontline Staff

Message	Description	What To Do
"ID has NOT been verified. Please ask customer for their physical Government issued photo ID."	The ID is an unsupported ID type, such as a military ID.	Ask visiting member for an acceptable form of ID.
"An error occurred authenticating your ID, please try relaunching the application within My Co-op."	Login from My Co-op failed.	Log in to My Co-op again.
"Your session has expired. Please relaunch the application from within My Co-op."	Login from My Co-op idled too long.	Log in to My Co-op again.
"Access code not recognized, please try again." "Error finding access code. Please try again."	Access code not found. Could be due to wrong number keyed in.	Confirm access code from member.

Message	Description	What To Do
"Access code expired"	Access code expired after 20 minutes.	Member needs to start verification process again.
"We could not generate an access code. Proceed to the teller."	May indicate fraud, or member inadvertently entered incorrect information.	Follow Shared Branch Operating Rules and Regulations.
"Something went wrong: an error occurred authenticating your ID, please try relaunching the application from within My Co-op."	Frontline staff will be unable to launch the IDCheck tile within My Co-op.	When an admin sets up frontline staff access through the Delegated Admin tile, all of the following fields must be completed: Select a Type User Name Email First and Last Name Admin level Springboard Org ID (the credit union's 4-digit identification number from us).
Frontline staff cannot get through PingOne validation, as the phone number on record is either outdated or incorrect.	Frontline staff receives an Authentication SMS sent to mobile 1(********##). The last 2 digits of the phone number will appear. If PingOne authentication is not completed, staff member will not be able to get into My Co-op.	Admin needs to submit a ticket through Client Service Delivery or your Client Growth Executive to Client Production Support internal inbox to update PingOne. Included in the request to Client Production Support should be the Frontline staff's current email, current mobile phone number, full name, credit union name, old phone number (if available) that needs to be removed, and any other information that would be helpful.

Reports

When your credit union activates IDCheck and begins using it, reports are available in the Insights Center for Shared Branch.

Report fields are the following:

- Date
- Time
- Member name
- ID type
- ID number
- Validation response – Pass, Reject, or Resubmit
- Reason Code – Details regarding the validation response

Daily Operational Reports

Daily operational reports contain data recorded as part of the transaction when an ID is scanned in IDCheck. You can use this information to research cases of fraud or suspected fraud.

Dashboard

The IDCheck dashboard contains higher-level aggregate information and does not contain any member data. For example, how many passes and fails occurred in a month, and how many transactions were performed with ID validations.

Shared Branch FAQ

What is IDCheck?
IDCheck Shared Branch is a product to help verify and prove a member's identity to effectively fight account takeover and identity theft for in-branch fraud.

Is every Shared Branch client required to join IDCheck?
As of May 1, 2025, all clients will be required to use IDCheck to verify members for withdrawal transactions that occur with out-of-state IDs. This requirement is aimed at addressing the most prevalent area where we observe account takeover fraud, which is with out-of-state IDs.

What scenario qualifies as an out-of-state ID withdrawal?
An out-of-state ID withdrawal is one where the ID that a member provides for verification is issued by a state other than the state they are in while completing the shared branch transaction.

Are core changes necessary?
There are no core changes necessary to use IDCheck.

Is IDCheck enrollment automatic or do credit unions need to take any action?
Enrollment in IDCheck is automatic. The only participation needed from credit unions as a part of this process is having admins set up frontline staff in My Co-op if they are an acquirer. Velera will send out more information regarding this process as the requirement date approaches.

How does IDCheck affect the liability when fraudulent transactions are successful?
IDCheck does not impact the liability system around fraudulent transactions. For more details, please refer to the Shared Branch Operating Rules and Regulations.

What is the technology behind IDCheck?
IDCheck is powered by Socure's DocV product. Socure's more than 2,400 clients include 17 of the top 20 banks, 13 of the top 15 credit card issuers, leading Buy Now, Pay Later (BNPL) providers, and over 500 fintech companies. The company's solutions are trusted by customers including Chime, SoFi, Robinhood, Green Dot and others.

Can acquirers choose to use IDCheck for other transaction types or suspicious transactions?
Yes, acquirers can use IDCheck for any transaction type, not just withdrawal transactions. They can even utilize IDCheck to verify their own members outside of the Shared Branch setting, if desired.

What is the price of IDCheck?
For pricing, contact your Velera representative, reference the email sent October 30, 2024, or ask your Shared Branch representative.

What is stored vs. un-stored validation pricing?
When members go through the IDCheck process for the first time, they are given the option to store their validation for future use. If they opt in to store the validation, each subsequent validation (with the same device and until their ID expires) will have reduced pricing. For additional information, reach out to your Velera representative, reference the email sent October 30, 2024, or ask your Shared Branch representative.

Are there estimated vendor costs?
There are no IDCheck vendor costs passed to the credit union.

How can credit unions get a sense of estimated cost and ROI of IDCheck?
The IDCheck Shared Branch LeveragePoint Tool is available, and a custom presentation of your estimates can be requested to your Velera point of contact.

How does a visiting member access IDCheck?
A visiting member scans the QR code with a smart device or smart phone.

Where does my credit union get a sign to display?
During the onboarding process, your credit union will receive a digital QR code to create a sign for in-branch use.

What should I do if IDCheck displays an error message?
Administrators can refer to the Troubleshooting and Error Messages section in this guide. Admins can also contact Client Service Delivery at 800-782-9042, option 3, or via clientcare@coop.org or your State Partner Representative.

What happens if a member does not have a smart phone?
A smart device is required for this service. If a member does not have a smart device, an option to consider would be having a credit union owned tablet or iPad available for members to use, given their policies and procedures. If a credit union tablet or iPad is used, the stored verification option should not be selected.

What happens if a member does not have an ID?
Visiting members must present valid identification. For additional information, refer to Shared Branch Operating Rules and Regulations on identifying a visiting member.

What happens if a member who was previously authenticated and opted in to storing their validation gets a new smart device?
The member needs to go through the verification process again since IDCheck correlates verification to the device.

What happens if a member who was previously authenticated and opted in to storing their validation has an expired ID?
The member needs to go through the verification process again.

If a visiting member's smart device has poor cellular connection, can IDCheck be used?
If a branch consistently has poor or no cell service, it is advised that the acquiring branch have available one or more smart devices connected to Wi-Fi that visiting members can use.

How do I access reports?
IDCheck reports are accessed in the Insights Center, where an Operational Report and a Dashboard Report with IDCheck activity are available.

Can military IDs be used?
Although a military ID is a valid ID in the teller line, military IDs are not supported in IDCheck due to a federal regulation that does not allow federal IDs to be copied or photographed. IDCheck will reject a military ID; photocopying any U.S. government identification is a violation of Title 18, US Code Part I, Chapter 33, Section 701. If the member does not have a valid non-military ID to present, an alternate verification method should be used.

What should we do if our credit union has adopted IDCheck, but it does not work right or our frontline staff can't access it?
Contact Client Service Delivery or your State Network Partner (SNP).

What information is stored, and how is it used?
Please refer to Socure's privacy policy: https://www.socure.com/privacy

How does frontline staff access IDCheck?
Frontline staff accesses IDCheck by selecting the app in My Co-op. The IDCheck admins at your credit union will ensure frontline staff is able to access IDCheck.

If a visiting member does not know their account number, what do they do?
Account number is required for a visiting member to use IDCheck. The visiting member will need to contact their home credit union (issuer credit union) for further assistance.

If IDCheck authenticates the member, but frontline staff does not think the person looks like the person in the picture, what should they do?
At the Verify ID screen, the frontline staff needs to select "No" when asked if the member is in front of them.

When an incorrect account number is entered by a visiting member, what happens?
Account information for frontline staff does not have a green circle with a check mark. An incorrect account number may or may not indicate fraud since the member may have accidentally entered a wrong number.

What happens if a visiting member enters their account number correctly, but their account number is not correct on the core?
A green circle with a checkmark does not appear by the account number on the Verify Information screen, indicating that data does not match.

Do tellers still need to write down information?
When IDCheck is used to verify a member, there is no need for the frontline staff to document the ID number on the receipt. The Shared Branch Operating Rules and Regulations contains more details on this.

Does a passport count as an out-of-state ID?
Since passports are federally issued, any withdrawal using a passport as verification qualifies as out of state and is subject to the IDCheck requirement.

Will this work with foreign passports?
Yes, IDCheck is capable of processing passports from many different countries.

Once saved, can a member edit the information they originally input during validation?
Yes, every time a stored member initiates the IDCheck process, they will have an opportunity to edit previously entered information.

If a member has accounts with two different credit unions, does the member need to go through the IDCheck process twice in order to conduct a transaction at each credit union?

IDCheck requires a member to select the credit union they are a part of at the beginning of the member workflow, so if they want to complete another transaction with a different credit union they will need to go through the process again and select the second credit union. Note, that this is only required if both transactions are withdrawals with out-of-state IDs.

What happens if a person opts in and then later claims their phone was stolen and used? Should the tellers still be checking physical IDs beyond just a code?

The Shared Branch Operating Rules and Regulations does not require frontline staff to check physical IDs if a valid access code is provided. Additionally, tellers are still presented with the image of the ID and selfie images uploaded during the process in My Co-op and are prompted to confirm that the person in front of them matches the images.

How does frontline staff access IDCheck?

Frontline staff accesses IDCheck by selecting the app in My Co-op. The My Co-op admins at each credit union are responsible for ensuring frontline staff have access to IDCheck.

How does an admin provide frontline staff with access to IDCheck in My Co-op?

For the IDCheck tile to appear in My Co-op for frontline staff, the My Co-op admin at the credit union ensures the user is added to the IDCheckbyCOOP group. For more information, see the interactive guide for admins in the email sent March 2025 with the Subject, "IDCheck: The Latest Updates, Resources, and Action Items".

Where does my credit union get a sign or other marketing material to display?

A member-facing marketing kit is available to all credit unions.

Contact Information

For assistance with IDCheck, you can contact any of the following:

- Your Client Growth Executive
- Client Service Delivery at 800-782-9042, option 3 or clientcare@coop.org
- Your State Partner Representative