MOP
Membership Opening Process

2023 Update

SecuriKey

MOBILE TECHNOLOGIES GROUP
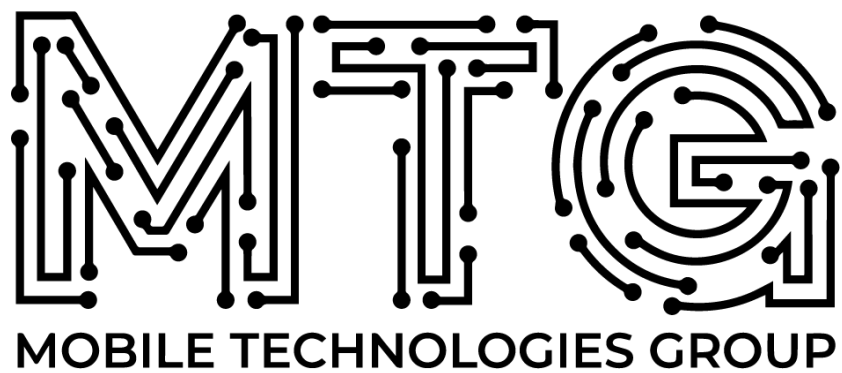
LEGAL DISCLAIMER
The information contained in this document does not constitute legal advice. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

MOP WEBSITE CONTROLS

Cross Site Forgery Prevention. Inputs are sanitized, and sessions tokens are used to prevent cross site forgery.

Session Timeout. The timeout is 5 minutes and activity based, meaning and if user has an idle screen for 3 minutes the user will get a popup advising 2 minutes are left. If the user maintains activity, the session will continually extend itself. Activity is mouse/keyboard actions on the active browser window.

MOP Restrictions based on Session. Users cannot jump ahead or go back on certain pages, and verify, fund, and enroll processes are restricted to single use (even when multiple windows are opened to the same page).

Dynamic API keys for External Access. Keys needed for external access to MOP change all the time, rather than a static set of keys that could be lost or stolen.

DATA TRANSMISSION

Encryption. Information entered by the applicant is encrypted through HTTPS during transit. TLS 1.2 is enabled and preferred. This is standard. Encryption will only fall back to TLS 1.1 and TLS 1.0 only if the member's browser does not support 1.2.

Data Storage. No member data is stored on the MOP servers. Member data is sent to CU*BASE after the verification process is completed.

PERSONAL VERIFICATION CONTROLS

Patriot Act Disclosures. Required Patriot Act disclosures are provided on the MOP site to the end user.

Precise ID Verification. Verification itself is provided by Experian Precise ID (a mandatory subscription required to use the MOP service).

OFAC/Blocked Persons. MOP includes an Experian Precise ID scan which asks the applicant questions to confirm their identity. This process also includes an OFAC scan. A record of the scan is saved in the Experian ID software. The membership OFAC Tracker will record the next time an OFAC scan is run on all your memberships.
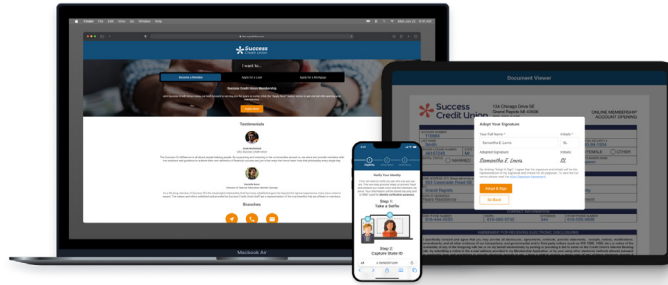
BIOMETRIC CONTROLS

Consent. Propsective members must consent to the use of their biometric information before sending the selfie. Information is sent and stored using encryption.

Retention. Biometric information is permanently deleted after 48 hours.

CU*ANSWERS

OVERVIEW:

MEMBERSHIP OPENING PROCESS ("MOP")

CU*Answers' online Membership Opening Process ("MOP") allows our network credit unions to conveniently enroll and verify new members from a user-friendly and attractive webpage. All required disclosures and identity verification steps are provided through this seamless MOP process. MOP is a secure method for enrolling new members online.

NEW FOR 2022-2023: MOP 3.0 allows credit unions to perform automated verification of new members by the use of a selfie and State ID. Registration can be performed by either through a desktop computer with a camera or by the members mobile phone or tablet. MOP 3.0 uses Daon, the provider of the same technology used to power MACO for Its Me 247 Mobile Banking logins.

In addition, MOP 3.0 allows geographical filtering by state to exclude individuals who are ineligible for membership.

USING SECURIKEY: Credit unions may be asked by examiners or auditors to provide a MOP risk assessment, documenting MOP's safeguarding of non-public personally identifiable information, and the requirements for member verification under the Patriot Act. **SecuriKey provides descriptions of the controls used to protect sensitive information and verify identity**.

ABOUT DAON: MOP 3.0 identification controls is provided through Daon, Inc., and their IdentityX product. Daon is based out of Ireland, and has a worldwide customer base, including government agencies.


SecuriKey

MOP WEBSITE CONTROLS

The webpage and its forms are protected through input sanitization and the use of session tokens. The user session will time out after five minutes of activity, with a warning popup to let the user know the session will be terminating. Users cannot jump ahead or go back to certain pages, and the enroll processes are restricted to single use (even if the user has multiple pages open). Information is encrypted through industry standards, and the MOP site does not store any user information. Information is passed directly to Experian Precise ID and stored securely within CU*BASE.

GEOGRAPHIC FILTERING CONTROLS

Credit unions can automatically filter and reject applications by state. Credit unions can configure MOP use CU*BASE Tool #13 'Work Online Banking Apps/Requests' allows the credit union to further review the rejected applications.
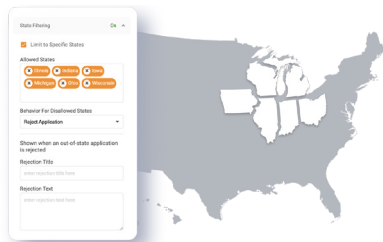
BIOMETRIC CONTROLS

Potential members are provided access to the Privacy Policy and must provide consent before sending their selfie and ID for verification. TLS v1.2 is used to protect information sent from the MOP website.   Identification document images are submitted to the AuthenticID platform for additional processing. AuthenticID uses only FIPS 140-2 algorithms with a default of AES-256 for symmetric encryption. Sensitive customer data, including document images, are encrypted while in transit and at rest. All binary data (images, templates, etc.) are AES-256 encrypted in the IdentityX database. Retention period is configured to be no more than 48 hours.

MOP ID VERIFICATION CONTROLS

MOP includes an Experian Precise ID scan which asks the applicant questions to confirm their identity. This process also includes an OFAC scan. A record of the scan is saved in the Experian ID software. The membership OFAC Tracker will record the next time an OFAC scan is run on all your memberships.

An online membership application can also end as a membership application to be worked in Tool #13. During the process of working the application and converting it to a membership, an OFAC scan is run. There is no OFAC record of this scan in the membership OFAC tracker because the member was still a non-member at the time the OFAC scan was run. Proof of this scan can be found using Tool #559: OFAC Non-Member Scan History. Look for the date range the membership was opened and OPEN NEW MEMBERSHIP will appear as the reason for the OFAC scan of the member. The Membership OFAC Tracker will record the next time an OFAC scan is run on all your memberships.

OFAC/BLOCKED PERSONS

Required Patriot Act disclosures are provided on the MOP site to the end user. Verification itself is provided by Experian Precise ID (a mandatory subscription required to use the MOP service). Credit unions can tweak these Experian rules to exclude questions or include different questions that can be asked. CU*Answers will help the credit union work with Experian if the institution requires assistance during this process. Credit unions can also optionally allow users to end the MOP session and request a "traditional" Member Application Process ("MAP").

If a prospective member does not pass the criteria for Experian Precise ID verification, CU*BASE Tool #13 'Work Online Banking Apps/Requests' allows the credit union to further review the application. If the member passes the first step of Experian Precise ID verification, the application is also run through the Blocked Persons database within CU*BASE. If there is a Blocked Persons match, this match will also be submitted to CU*BASE under Tool #13 'Work Online Banking Apps/Requests'.

ACCOUNT OPENING AND ONLINE BANKING

Once Experian Precise ID verification and Blocked Persons checks are passed, members may now open accounts and fund the base share account through the Card Services product with Magic Wrighter. Once a member completes their deposit, Magic Wrighter converts this transaction to ACH and the credit union will receive the deposit through their daily ACH processing. Once the new member works through all the steps registering through MOP, the member with a click may go directly to Online Banking within It's Me 247 (desktop & mobile).

CU*BASE Tools all the credit union to configure forms to send to new members for compliance requirements such as Truth in Savings and eSign.
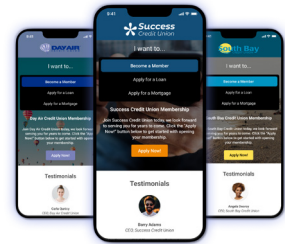
MOP WEBSITE	BIOMETRIC IDENTIFICATION	OFAC
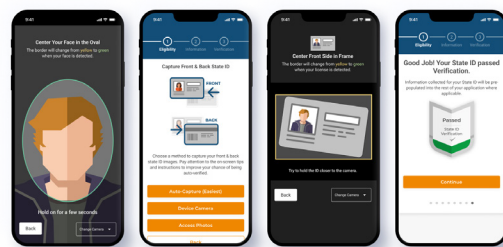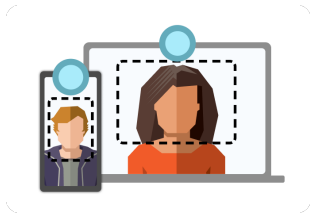
Santized Inputs
Cross Site Forgery Prevention
Location Filtering (optional)
Session Timeout
Restructions Baed on Sessions

Policy and Consent Form
Sent by TLS v 1.2
AES-256 Encryption
Limited Retention

Disclosures Provided
Configurable
OFAC Scan Run
Compared to Block Persons

ENCRYPTION

Information entered by the applicant is encrypted through HTTPS during transit. TLS 1.2 is enabled and preferred. Encryption falls back to TLS 1.1 and TLS 1.0 only if the user's browser does not support 1.2.

CROSS SITE FORGERY PREVENTION

Inputs are sanitized, and sessions tokens are used to prevent cross site forgery.

LOCATION FILTERING

Optional control to reject applications by states.

SESSION TIMEOUT

The timeout is 5 minutes and activity based, meaning and if user has an idle screen for 3 minutes the user will get a popup advising 2 minutes are left. If the user maintains activity, the session will continually extend itself. Activity is mouse/keyboard actions on the active browser window.

MOP RESTRICTIONS BASED ON SESSIONS

Users cannot jump ahead or go back on certain pages, and verify, fund and enroll processes are restricted to single use (even when multiple windows opened to same page).

DYNAMIC API KEYS FOR EXTERNAL ACCESS

Keys needed for external access to MOP change all the time, rather than a static set of keys that could be lost or stolen.

DATA STORAGE AND DESTRUCTION

Protected by AES-256 Encryption during the ID verification process. Data is destroyed within 48 hours of the application process.

OFAC

Disclosures are provided to applicants prior to Experian Precise ID verification. OFAC scans are run prior to offering membership. Applications will be compared to the credit union's Block Persons database.
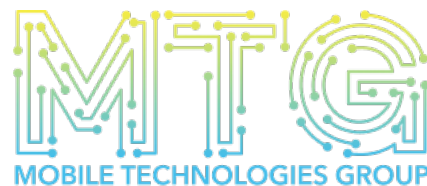
VERSION CONTROL

VERSION	DATE	CHANGE	TEAM
1.0	June 14, 2018	First published	Internal Audit
2.0	May 23, 2021	Revised for clarity	Internal Audit
3.0	January 30, 2023	Updated for MOP 3.0	Internal Audit

LEARN MORE

CONCERNS ABOUT BSA?

AuditLink can provide support for CU*BASE security and tool options.

KEEP CURRENT ON LATEST ENHANCEMENTS

All the latest updates for CU*BASE can be found on our Kitchen page.