JUNE 2018
Version 1.0

SecuriKey

CU*ANSWERS

Risk Assessment for MACO

Multi-Authentication Convenience Option

CU*ANSWERS
A Credit Union Service Organization

CONTENTS

LEGAL DISCLAIMER

INTRODUCTION

CU*Answers' Multi-Authentication Convenience Option ("MACO") allows our network credit unions to provide your members more options for authentication in **It's Me 247** Mobile Banking. MACO includes four convenience options: fingerprint, face recognition, voice recognition, and PIN.

Credit unions may be asked by examiners or auditors to provide a MACO risk assessment, documenting MACO's safeguarding of authentication information. Members may have concerns about biometric information used for authentication.

CU*Answers does not recommend advertising MACO as being "more secure." **MACO is secure** but is primarily a convenience option for members.

QUICK REFERENCE

MACO

Online Banking Authentication: Members cannot use MACO unless initially authenticated through Online Banking.

Authentication Process: Biometric authentication is a process, requiring the member to ensure identity recognition prior to authentication with the Mobile Banking system.

DATA TRANSMISSION

Encryption: Information entered by the member is encrypted through 256-bit encryption.

Data Storage: No biometric data is stored on the MACO servers. Any biometric authentication information is stored on the member's device using the device's native encryption (not in the app itself).

AUTHENTICATION CONTROLS

Temporary/Permanent Lockout: MACO is temporary locked out if the member fails authentication. If member fails four times, the lockout is permanent.

Probabilistic Authentication: If biometric, authentication is provided through a probabilistic authentication algorithm.

INTERNET RETAILER SUPPORT CENTER

Learn more online at the Internet Retailer Support Center.

FEATURES

Four options: fingerprint, face recognition, voice recognition, PIN	**Biometric information is stored on the device, not on the authentication system**	**Members must authenticate with Online Banking before using MACO**

RISK ASSESSMENT TOOLS

Overview of MACO Security Features

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

Fingerprint. Fingerprint authentication will only show on devices that support fingerprint technology. 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 the member has 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.

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. 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 MACO server. If the photo metric matches what is saved on the MACO 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.

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.

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.

Authentication Information

Authentication information entered by the member is encrypted. Transmission security is provided by using 256-bit encryption. For fingerprint, voice, and face recognition, the credential information is compared against the MACO probabilistic algorithm on the server. If there is a match, the member is authenticated. **No biometric data is stored on the MACO servers**. The biometric information is stored encrypted on the member device through the native encryption of the device OS, not the MACO application. Credit unions and members who wish to know more about device native encryption can review options provided by the manufacturer of the device.

Members should not use MACO on a device that is shared. If a member loses the device, MACO can be removed on all devices by creating a new profile on a device. If this is not an option, the credit union can request CU*Answers to disable the profile.

Failed authentications will lock out MACO authentication for a temporary time. Standard login is still available if the account is locked out. The lockout time increases with each lockout. Members will be unable to use MACO for fifteen minutes, then twenty and then twenty-five minutes. At the fourth lockout, the MACO profile will be disabled.

About Daon

MACO is provided through Daon. Daon is based out of Ireland, and has a worldwide customer base, including government agencies. Many of their clients include international banks that use their products for mobile authentication, in the same way used in the CU*Answers Mobile Banking solution.

FEATURE MATRIX

To help you assess MACO security controls, we have developed a Product Feature Matrix that lists the security features of MACO.

Authentication Process	Encryption in Transit	Data Storage
Members must be authenticated through a standard login to Mobile Banking before using MACO *Members go through a process with biometric identifiers to ensure high degree of accuracy in authentication* *Members can de-enroll if the device is lost or stolen; MACO is not recommended if the member shares the device*	*Authentication information is transmitted using 256-bit encryption*	*Biometric information is not stored on the MACO servers; encrypted on the device using the device's native encryption (in the OS, not the app)*

VERSION CONTROL

VERSION	DATE	CHANGE	TEAM
1.0	June 14, 2018	First Published	Internal Audit