

# Strategies for Securing and Controlling Member Access



## INTRODUCTION

This booklet covers the strategic decisions your credit union should make to secure and control member access to **It's Me 247**. Included are issues relating to the configuration and management of member passwords, activation settings, tools for members, and ways to monitor activity.

## CONTENTS

SECURITY OVERVIEW	3
LAYERED SECURITY THROUGH THE PIB PROFILE	4
MINIMUM USAGE REQUIREMENTS	5
ACCESS TERMINOLOGY TO LEARN	6
CONTROLS FOR ACCESS TO ONLINE BANKING	9
PASSWORD CONTROLS	9
ADDITIONAL SECURITY FEATURES ON ENTRY	9
PASSWORD EXPIRATION/RESET RULES	10
ONLINE/MOBILE FRAUD BLOCK LIST	11
SECURITY DECISIONS TO MAKE	13
TO ACTIVATE OR NOT TO ACTIVATE?	18
ACTIVATE/DEACTIVATE VIA MEMBER PERSONAL BANKER	18
ONLINE/MOBILE PASSWORD AND SECURITY SETTINGS/MFA CONFIGURATION	19
CONFIGURATION OPTIONS FOR FIRST TIME USER MFA AND SECURITY SETTINGS	21
CONFIGURATION OPTIONS FOR STANDARD LOGIN MFA	23
MFA ONE-TIME PASSCODE AND REGISTRATION AT ONLINE BANKING LOGIN	24

**Revision date: February 17, 2025**

For an updated copy of this booklet, check out the "It's Me 247" Reference page of our website:  
<http://www.cuanswers.com/resources/doc/its-me-247-reference/>  
CU\*BASE® is a registered trademark of CU\*Answers, Inc.

MFA FOR NEW MEMBERSHIPS	26
MFA FOR PAY ANYONE OR PERSONAL INFORMATION UPDATE	28
“TRY IT BEFORE YOU BUY IT!” – PROMOTIONAL CAMPAIGNS	30
PROMOTIONAL CAMPAIGN CONFIGURATION	31
MESSAGING ON ENTRY EXPLAINS REASON MEMBER NEEDS RESET	35
INCORRECT PASSWORD ENTRIES RESET	35
RESET FOR THREE INCORRECT SECURITY QUESTION ANSWERS	36
RESET PASSWORD EXPIRED DUE TO NON-USE	38
USERNAMES	39
OPTIONAL USERNAME	39
REQUIRED USERNAMES	40
ASSISTING A MEMBER WITH A USERNAME IN CU*BASE	41
STATEMENT SECURITY	43
ONLINE BANKING INDEMNIFICATION NOT REQUIRED FOR eSTATEMENTS	43
BATCH MEMBER UN-ENROLLMENT	43
TIMEOUT NOTIFICATION	44
PASSWORD CHANGE REMINDERS	45
PERSONAL INFORMATION CHANGE NOTIFICATIONS	47
CHANGES TO ONLINE BANKING PASSWORD AND EMAIL	47
PERSONAL INFORMATION CHANGES	48
RED FLAG WARNINGS IN CU*BASE FOR EMPLOYEES	48
JUMP ACCESS CONTROLS	50
INTER-MEMBER TRANSFER CONTROLS	51
OVERVIEW	51
TRANSFER CONTROL LISTS	51
DIRECT ACCOUNT INPUT	51
INTER-MEMBER TRANSFERS: WHAT THE MEMBER SEES IN ONLINE BANKING	52
EVALUATING THE REASON FOR A PASSWORD CHANGE	53
EVALUATING YOUR MEMBERSHIPS WITHOUT ACTIVITY	54
REVIEW YOUR CREDIT UNION PLAN AND PROCEDURES	54
APPENDIX A: ONLINE BANKING USE AGREEMENT	55

---

# SECURITY OVERVIEW

**It's Me 247** is an online banking product that has been designed to safeguard your members' money and privacy by using the latest Internet security technologies. To further ensure security, these protective technologies have been applied in layers to address each phase of the online transaction.

Transmission security is provided by using 2048b-bit SSL encryption, ensuring that only the member and the **It's Me 247** systems are able to read the transaction information as it flows across the Internet. Through our use of digital certification, the member also can be assured that they are communicating with the legitimate **It's Me 247** server, and not an imposter.

User account security is furnished through the use of a unique Member Account Number (or username), and a combination of password and security question answer known only to the member. Without this information: account number (or username), password and security question answer, accessing account data and initiating transactions online is impossible.

**About usernames:** Members can optionally select to create a username. Then the member uses this username in place of their account number when they log into online banking. Credit unions can elect to require usernames. In this case this feature is not optional, and all members must set up usernames to use in place of their account number. See **Page 39** for more information about usernames.

- **Rules for Usernames:** Usernames can contain all letters, or a combination of letters and numbers. They can contain spaces, but not special characters. They are not case-sensitive. Usernames cannot contain the account number, nor the member's first or last name. Usernames can be a maximum of twenty characters.

Once the member has set up a username, they can change at any time in online banking, but they can't clear it. Credit union employees cannot create usernames for members. However, CU\*BASE does have a feature to clear the username so that the member is prompted again for a new one.

Credit unions can require that members set up usernames. This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

**About passwords:** Password retries are limited to 3, at which time the password is deactivated, and the member must contact the credit union for reactivation. Credit unions can select a minimum number of characters for passwords (minimum password length of six characters, up to a maximum of ten). If desired, credit unions can force members to follow **complex password** rules (requires three of the four following: uppercase letter, lowercase letter, number, and special character).

Access security is provided by a combination of segregated network architecture, hardened server configurations, and redundant firewalls. Our segregated network architecture separates the **It's Me 247** servers from the systems that contain member data. Consequently, member data may only be exchanged between these systems through the use of a valid member request following verification of Member Account Number and PIN/password. Internet-based attacks (hackers) are stopped through the

use of redundant state-of-the-art firewall technology and hardened server configurations.

To further ensure that **It's Me 247** security measures continue to meet the ever-changing security threats of the Internet, **It's Me 247** is reviewed on an ongoing basis by regulators and expert security consultants, and monitored by CU\*Answers network engineers.

**About security questions:** When logging into online banking for the first time, members must set up 3 security/challenge questions. These can be used to reset the member's password in the event that they have forgotten their password. To log in to online banking, members must enter their password *and* answer one of the three questions they set up. Answers can be a maximum of thirty characters.

**A Note About Security Questions:** For maximum security, members can choose to use their security questions as a second, longer "passphrase." A passphrase is essentially a sentence used for the purposes of a password and due to its length is much harder for hackers to guess. "A passphrase is hard to guess!" is exactly 30 characters, and according to some sites, would take a hacker over a billion years to crack! For members or examiners concerned about password security, recommend that they use their security questions as a secondary passphrase.

## LAYERED SECURITY THROUGH THE PIB PROFILE



As a companion to the security features already available in **It's Me 247**, we also offer an optional layered security approach which can be activated as a companion to **It's Me 247**. A Personal Internet Branch (PIB) Profile lets your members assume only the risks they are comfortable assuming on the Internet, and allows for additional layers of security for selected transaction types, such as inter-member transfers, updating personal information, and accessing the EasyPay online bill pay system. For a list of **It's Me 247** features that can be controlled via the PIB Profile, refer to the **It's Me 247** Features List.

For complete details about implementing PIB, refer to the "**It's Me 247** Personal Internet Branch (PIB)" configuration and user guide booklet as well as the flyer, "Implementing PIB: Rollout Strategies A to Z." Both are available on our website at [www.cuanswers.com/client\\_reference.php](http://www.cuanswers.com/client_reference.php).

## MINIMUM USAGE REQUIREMENTS

Remember that as security requirements and the Internet world change, so will these requirements. If a member is having trouble accessing **It's Me 247** features, the first step is always to upgrade the browser software.

- Supported browsers are the two latest versions of: Chrome, Firefox, and Edge, and Safari.

Modern browsers provide features and benefits that older browsers may not:

- CSS3
- HTML5
- Faster Speed
- Safer Protection
- Continued Support from major vendors

Older/legacy browsers can also cause problems with websites and applications you use frequently. In these older browsers you may have trouble using certain features in **It's Me 247** Online Banking.

- NOTE: Because phones can vary, desktop **It's Me 247** features are not warranted on mobile devices. For best results, use a computer with desktop **It's Me 247**.

---

# ACCESS TERMINOLOGY TO LEARN

The following terms explain controls on a member's access to **It's Me 247** that are used within this publication.

**Activate / Deactivate / Activation flag** – Refers to the activate Online Banking flag that is turned on to allow a member to access his/her account through online banking. If turned off, the member cannot use the system at all. This is controlled via **Tool #72 Update ARU/Online Banking Access** or through **Tool #14 Member Personal Banker**.

**Complex Passwords** – If you have not already done so, your credit union has the option to force your members to make complex passwords. Complex passwords rules require three of the four following: uppercase letter, lowercase letter, number, and special character. Once you activate this feature, members without complex passwords will need to change their password to be complex the next time they log in. This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

**Custom PIN or Password** – Your credit union can allow credit union employees to enter a custom password for the member via **Tool #14 Member Personal Banker** or via **Tool #72 Update ARU/Online Banking Access**. These passwords are not temporary. They do not expire like temporary passwords. (See below.) This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

**Disable** - Refers to when a member tries to access online banking with an incorrect password/security question combination 3 times in a row. In this case, the actual password on the member's record is cleared and must be reset to a temporary password by an MSR in order to get back into **It's Me 247**. **This has no effect on the actual Activation flag.** When the MSR changes the member's password via **Tool #14 Member Personal Banker**, he or she will see a messaging window (see page 35) explaining the reason for the lack of access and will be able to reset the password from this screen. The member could also use the "I forgot my password" feature in **It's Me 247** and answer his or her security questions to accomplish this. Passwords can also be reset via **Tool #72 Update ARU/Online Banking Access**.

**Expired Due to Non-Use (Stale Password)** - Refers to when a member has not used **It's Me 247** for a period, determined by the expiration period (in days) in the *Online/Mobile Password and Security Settings*. (See page 19.) The expiration period is measured by evaluating the member's *Last Logged In Date* every time he/she attempts to log in. **This has no effect on the password itself or the Activation flag.** When using **Tool #14 Member Personal Banker**, the MSR will receive messaging (see page 35) alerting him or her to the reason for the blocked access and will be able to reset the member's password to a temporary password. Passwords can also be reset via **Tool #72 Update ARU/Online Banking Access**. Passwords can be set to expire after 1-90 days of non-use. (Or the credit union can select 999 days to never expire passwords due to non-use.)

**Hide My Typing** – Members can use this option and click and eyeball symbol to type asterisks when entering the answer to a security

question when logging on to **It's Me 247**. (See following entry on Security Questions.)

**Inter-Member Transfers** – Inter-Member Transfers allow members to transfer to other members at your credit union. These transfers are done via the Transfer Wizard in online banking. Two options exist for inter-member transfers, and the credit union can select to allow one or both options. See page 51 for more information.

**Maximum Password Length/Minimum Password Length** – The maximum length a member's password is set by the system at 256 characters. The minimum length is set by the credit union and must be six to ten characters. This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

**Multi-Factor Authentication (MFA)** – *See also Two-Factor Authentication.* Credit unions can require that a member have enter a code texted or emailed to them for a secondary authentication to access certain online banking features such as during standard login, during first-time authentication (also known as Method B), when making Pay Anyone (Person-to-Person transfer services), or when updating their personal information. See pages 19.

**Promotional Campaign** - Credit unions can run promotional campaigns to encourage members who fit certain requirements to take it for a “test drive.” See following promotional campaign section (beginning on page 30) for directions on setting up and running a promotional campaign.

**Reset** - Refers to having an MSR take the option that changes the member's password to the temporary password setting. The system will require the member to change the password immediately upon login.

**Jump** – Once this feature is activated, and the appropriate permissions are given, the member can login to one membership and from there the member can “Jump” to another account (for almost full permissions). See page 50 for details.

**Security Questions** – Refers to the question the member is presented (in conjunction with a password request) each time he or she logs into **It's Me 247**. Members select these questions and answers the first time they log into online banking. When the member forgets his or her answers, a Member Service representative can delete the questions and answers in CU\*BASE (first following credit union policies). In this case, the member can login and setup the questions and answers again. Security questions can be a maximum of thirty characters, allowing you to create a phrase as an answer. When a member locks themselves out of online banking with three incorrect password attempts, they can use the “I forgot my password” feature and to be able to reset their password. They must answer all three security questions correctly.

[My member is trying to log into online banking and their security question does not work. Why might that be the case?](#)

**Special Character** – Refer to one of the options to strengthen a password for complex passwords. Members must use three of the following: lower case letter, upper case letter, number, and special character. Some special characters are not permitted because they are used by certain programming languages. Permitted special characters are listed on

the password change screen and the screen where the security questions and answers are set up.

Learn more in this Answer Book item: [What special characters are allowed in online banking passwords, security question answers, and personalized security questions? Which ones are not allowed?](#)

**Temporary Password** – Members get a “temporary password” any time the credit union grants them access, including password reset, new member password, or password for promotional campaign. The length of time this password is valid depends on the method by which the password is set. (See following section.) Credit unions have four configurations to select from for their temporary password, including:

- Last four digits of SSN (current option)
- First four digits of SSN and last two letters of last name (all CAPS)
- 4-digit birth year and first two letters of last name (all CAPS)
- Last four digits of SSN and 4-digit birth year

This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.) *NOTE: The new temporary password is used with Method A. See page 19 for more details.*

**Transfer Control List** – Transfer control lists can be used to control to which memberships (at your credit union) that a member can transfer to via the Transfer Wizard, as well as the accounts used for ACH Distribution, and Automated Funds Transfer (AFTs) set up by the member in online banking. This list also dictates transfers made via Mobile Web Banking; Credit unions control the addition of memberships to this list. See page 51 for more information.

**Two-Factor Authentication** – Members may be asked to authenticate by entering a code that is texted or emailed to them. This feature is available as one option for first time login. This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

You may also require this type of authentication two access certain features within **It's Me 247** once the member logs in. (See page 24)

**Two-Factor Authentication** – See Multi-Factor Authentication.

**Username** – Members can create a username while in **It's Me 247** that can be used in place of the account number at login. Credit unions can elect to require usernames. In this case, the feature is not optional, and all members must create a username. Requiring usernames is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

Usernames can be a maximum of twenty characters. Refer to Page 3 for rules when creating usernames. Refer to Page 39 for more information about usernames.



---

# CONTROLS FOR ACCESS TO ONLINE BANKING

## PASSWORD CONTROLS

In light of the increasingly security-conscious environment of the Internet, **It's Me 247** Online Banking offers many controls for managing the passwords used by members to gain access to their accounts.

In general, the longer and more complex a password is, the more difficult it is for an unauthorized person to compromise it. Remember that online banking provides access to information that can be used for identity theft (such as address, phone, and email). Online Banking mitigates this risk by limiting the number of times someone can attempt to guess a password (3 incorrect attempts and the password is disabled), as well as requiring that a security question be answered each time the member logs in.

- ◆ Online banking passwords can be up to **256 alphanumeric characters**, including special characters
- ◆ Passwords are **case-sensitive** (i.e., Ds443&sld is different from dS443&SLD)
- ◆ Passwords can include a blank space
- ◆ You specify a **minimum number of characters** (At least 6 to 10 characters are recommended, six characters are required) This is set in the *Online/Mobile Password and Security Settings*. (See page 19.)
- ◆ If desired, you can force members to follow **complex password** rules (requires three of the four following: uppercase letter, lowercase letter, number, and special character). This is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

NOTE: Certain special characters are not allowed because they are used by special programming languages. The available special characters are listed on the password change screen. Learn more in this Answer Book item: [What special characters are allowed in online banking passwords, security question answers, and personalized security questions? Which ones are not allowed?](#)

## ADDITIONAL SECURITY FEATURES ON ENTRY

- **It's Me 247** requires users to answer a **challenge question** in addition to supplying a password each time they login to online banking. Members set up these questions and answers the first time they use online banking. Since answers can be a maximum of 30 characters, this gives the member an opportunity to create a longer, harder to guess passphrase to work in tandem with the password.
  - **NOTE:** These security question answers and customized security questions cannot have certain special characters in them. Refer to the Answer Book item above for more information.

- A member can create an *optional* **username** while in **It's Me 247** that the member can use *in place of* the account number when he or she logs into online banking. Usernames can contain a letters or a combination of letters and numbers. They are not case sensitive and can include spaces and cannot contain special characters. Usernames cannot contain the account number, not the member's first and last name.
- **Credit unions can elect to require usernames.** In this case all members must create a username (either as part of the initial login process or the next time they login. Then going forward, members log into online banking using their username in place of the account number. Requiring usernames is activated in the *Online/Mobile Password and Security Settings*. (See page 19.)

Refer to Page 3 for rules when creating usernames. Refer to Page 39 for more information about usernames.

## PASSWORD EXPIRATION/RESET RULES

Additional access controls are in place to control the length of time a temporary or unused password is available to the member without their logging into **It's Me 247**. If a member fails to log into **It's Me 247** within the allowed time, the member will need to call the credit union to reset the password for access.

- ◆ Credit unions have four configurations to select from for their temporary password, including: Last four digits of SSN (current option), First four digits of SSN and last two letters of last name (all CAPS), 4-digit birth year and first two letters of last name (all CAPS), Last four digits of SSN and 4 digit birth year. This is set in the *Online/Mobile Password and Security Settings*. (See page 19.)
- ◆ Members can request at any time that the credit union reset their password. They can always use the "I forgot my password" feature and answer their three security questions to reset their password. There are situations where they will need credit union assistance, however; for example, if they enter their security questions incorrectly three times.
  - ◆ **After following credit union policy, the member service representative can reset the password** using **Tool #14 Member Personal Banker**. When the member's password is reset using this screen, the temporary password is **valid for 24 hours**. After this period, the member must call the credit union for another reset. Members who log into **It's Me 247** will be required to immediately change their online banking password.
- ◆ If you select to enroll new members in **It's Me 247** when they open a **membership**, your credit union can select how long a period (**from one to seven days**) that the new member temporary password is valid. If the member fails to log into **It's Me 247** within this time frame, the member will need to call the credit union to reset it. Members who log into **It's Me 247** will be required to immediately change their online banking password. The number of days is set in the *Online/Mobile Password and Security Settings*. (See page 19.)

- ◆ **Online banking passwords can be configured to expire after a certain period of non-use.** Enter a configured number of days (1-90). (Or enter 999 days to never expire passwords due to non-use.) If a member does not log into online banking during this period, the member's password will expire due to non-use. **NOTE:** If a member logs into online banking at least one time during this period, the member's password will never expire.) This is set in the *Online/Mobile Password and Security Settings*. (See page 19.)

This expiration comes into play only after a member has not logged into **It's Me 247** for a certain period. This provides an extra measure of security for dormant memberships or members who do not choose to use your self-service options. If someone attempts to access the member's account after the expiration period, the application displays a message instructing the user to contact the credit union to reactivate the password. Similar to your credit union's dormancy procedures, we designed this feature to help limit the risk that an unauthorized person could access an unused account.

**It's Me 247** monitors authorization every time a member attempts to log in and controls access by comparing the last date the member logged in with the date to the configured expiration period. Remember that you can also choose to disable an individual member's access to these systems completely.

- **NOTE:** In your credit union's *Online/Mobile Password and Security Settings* (covered on page 19), your credit union does have the option to set online banking passwords to never expire. With this configuration, members' passwords will never expire due to non-use.
- ◆ You can choose to define a **promotional period** to allow selected active members to try **It's Me 247** for the first time or start up again if their usage has dropped off after a period. Refer to page 30 for more information on the setting up a promotional campaign.

These security features offer peace of mind for your members—with CU\*BASE tools that make it easy for your MSRs to help your members! In today's environment, there really is no better way to go.

## ONLINE/MOBILE FRAUD BLOCK LIST

Fraud Block Lists are accessed via **Tool 892 Fraud Block List/Blocked Persons List**.

If a person or organization is added to the online/mobile denial of service block list, an employee cannot enroll any membership with this SSN/TIN into online banking via the Member Personal Banker, during the membership open process (for example via Tool #3), or directly via PIN shortcut. When they try to check the "Online Banking" checkbox on the Audio/Online Banking screen, they will see messaging that the "SSN/TIN appears on block list."

- Because of this, the member will not be able to login to online or mobile banking, unless the member has previously been given access and has logged in already.
- Being on the block list does not affect access made prior to the addition to the block list. If the member is already enrolled in online banking, the addition to the block list will not prevent the member

from logging into that account *with the already created access points*. If a member on the block list has already logged into online banking, is subsequently added to the block list, and then tries to login using mobile banking (a new method of login they haven't used before), the member will be blocked from logging in via Mobile Banking.

If a match is found on a block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the membership from the appropriate block list.)

- NOTE: If a member has already logged in to their account, next block further access to the account. Uncheck Online Banking (and give a reason code), on the *Update Audio/Online Access* screen. This screen is accessed via the PIN shortcut or **Tool #14 Member Personal Banker**, then *Online Banking/ARU (activate, change PIN/Password; view access history)*.

Learn more in online help [Overview: Fraud Block Lists](#).

# SECURITY DECISIONS TO MAKE

Whether you are launching **It's Me 247** for the first time or trying to establish a sound strategy for managing member passwords and access to **It's Me 247**, use the following checklist to make sure you have covered all the bases. Many are activated or set in the *Online/Mobile Password and Security Settings*. (See page 19.) If you would like to make any changes to other of your configuration settings, or would like to discuss the options further, contact a Client Service Representative or use the **It's Me 247** Configuration Change Request Form available on our web site ([http://www.cuanswers.com/client\\_reference.php](http://www.cuanswers.com/client_reference.php)).

- **More information about these decisions is included in the rest of this document.**

<i>Decision</i>	<i>Choices Offered by It's Me 247 / CU*BASE</i>	<i>For configuration...</i>
<b>Activation Settings</b>		
Will multi-factor authentication (MFA) code or temporary password be used during first time-login?	<p>Credit unions can select from Method A or Method B to control a member's first-time login experience.</p> <p>Method A: The member logs in using their account number and temporary password, based on rules set by the credit union. <i>See below on temporary password.</i></p> <p>Method B: The member logs in using their account number and social security number. This prompts them to have a code sent to a phone or email associated to the membership, for a multi-factor authentication experience.</p> <p>Once the temporary password or code is entered, the member experience follows a similar pattern.</p>	<p>This is activated in the <i>Online/Mobile Password and Security Settings</i>. (See page 19.)</p> <p><i>Pictures of the member's experience of Method B are shown starting on page 24.</i></p>
Will multi-factor authentication be used for login and registration of devices?	<p>Credit unions can elect activate two-factor authentication and send a passcode via text or email when the member logs into online banking. Members also have the option of registering their devices, so they can skip MFA upon login for the configured number of days for that device.</p> <p>Members will enter the code on the second screen, and then the member experience follows a similar pattern.</p>	<p>This is activated in the <i>Online/Mobile Password and Security Settings</i> on the second configuration screen. (See section starting on page 19.)</p> <p><i>Pictures of the member's experience are shown starting on page 24.)</i></p>
What should the temporary password setting be for the credit union?	<p>Members get a "temporary password" any time the credit union grants them access without specifically setting a custom password, such as from a password reset, new member enrollment activation via Method A (see previous page), or promotional campaign). Credit unions have four configurations to select from for their temporary password, including:</p> <ul style="list-style-type: none"> <li>• Last four digits of SSN (current option)</li> </ul>	<p>This is activated in the <i>Online/Mobile Password and Security Settings</i>. (See page 19.)</p>

Decision	Choices Offered by <b>It's Me 247</b> / CU*BASE	For configuration...
	<ul style="list-style-type: none"> <li>First four digits of SSN and last two letters of last name (all CAPS)</li> <li>Birth year and first two letters of last name (all CAPS)</li> <li>Last four digits of SSN and birth year</li> </ul>	
Should usernames be required?	<p>Your credit union can elect to require usernames be used in place of account numbers when logging into online banking.</p> <ul style="list-style-type: none"> <li>In this case all members must create a username (either as part of the initial login process or the next time they login).</li> <li>Then going forward, members logging into online banking use their username in place of the account number.</li> <li>Members create usernames in online banking. Usernames can be viewed and deleted in CU*BASE but cannot be added for the member.</li> </ul>	<p>For newly converting credit unions, talk to your Conversion Coordinator about the desired setting when your credit union switches to CU*BASE and <b>It's Me 247</b>.</p> <p>This is activated in the <i>Online/Mobile Password and Security Settings</i>. (See page 19.)</p> <p><i>Refer to Page 3 for rules when creating usernames.</i>  <i>Refer to Page 39 for more information about usernames.</i></p>
Should all existing memberships be activated automatically?	<ul style="list-style-type: none"> <li>By default, all existing enrollment passwords are set to the temporary password setting for the credit union; members are required to change the password after logging in for the first time (must be something different than the default).</li> <li>This is done via promotional period for Method A.</li> <li>For Method B, as long as the member does not have security questions set up, they can enroll in the standard Method B method. See page 24.</li> </ul> <p><b>IMPORTANT:</b> <i>Remember that if you do not activate members, the promotional features will only apply to members who have been activated, but then do not use <b>It's Me 247</b> actively. Running a promotion will NOT work for the rest of your membership because the member activation flags will have been turned off. Therefore, we recommend you activate all then control access with new member password controls or deactivate all and only use expiration for controlling inactive members.</i></p>	<p>For newly converting credit unions, talk to your Conversion Coordinator about the desired setting when your credit union switches to CU*BASE and <b>It's Me 247</b></p> <p>For existing credit unions, contact Client Services for information about custom programming to “flood” the activation flag setting for all your memberships</p>
Should <u>new</u> members automatically be granted access and given a password?	<ul style="list-style-type: none"> <li>Used with Method A. (See activation settings section on the previous page.)</li> <li>Configure whether to activate online banking automatically for new memberships.</li> <li>If all new members are granted access, the number of days a new member password is active is configurable. See the Password section.</li> </ul>	<p>Contact Client Services to change the activation setting for new memberships. (Days for password to be active are controlled by the credit union.) This is set in the <i>Online/Mobile Password</i></p>

Decision	Choices Offered by <b>It's Me 247</b> / CU*BASE	For configuration... and Security Settings. (See page 19.)
If members are not automatically activated, how do they become activated?	<ul style="list-style-type: none"> <li>Develop an internal policy and procedure MSRs and phone staff can use to sell online banking and activate the new member's account.</li> <li>Give staff tips for talking to members - for example, ask members whether they want the option to use online banking whenever they are ready, sign up now, or disable the account so it cannot be accessed via <b>It's Me 247</b> until requested.</li> </ul> <p><i>HINT: You may even want to set up a workstation in the lobby that members can use to change their password right away.</i></p>	Use <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b> to activate a member's account
What if a member misuses the system or requests that no access be allowed to his accounts via online banking?	<ul style="list-style-type: none"> <li>Any member account can be permanently disabled from either online banking or audio response, or both</li> </ul>	Use <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b> and change the activation flag to disable an account
<b>Passwords</b>		
Do you want to force complex password rules?	<ul style="list-style-type: none"> <li>Activate the complex passwords flag</li> </ul>	This is activated in the <i>Online/Mobile Password and Security Settings</i> . (See page 19.)
What should your expiration period be for members who do <u>not</u> use <b>It's Me 247</b> regularly?	<ul style="list-style-type: none"> <li>Configure expiration period by number of days (1-90 days, for example 60 days). (Select 999 for never to expire.)</li> <li>If expired member tries to log in, will be notified as follows: <b>It has been more than xx days since you last logged in. Your password has expired. Please contact the Credit Union to reactivate your password.</b></li> <li>MSR can reset the password to the temporary password setting of the credit union. The member will have 24 hours to log in and will be required to change the password at this time.</li> </ul>	<p>This is set in the <i>Online/Mobile Password and Security Settings</i>. (See page 19.)</p> <p>To reset an expired member's password to the temporary password the MSR will use <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b></p>
Would you like to activate all members to start, but then "close" the enrollment period after a period of 1-7 days?	<ul style="list-style-type: none"> <li>Check to activate all online banking enrollments; also activate all new memberships automatically.</li> <li>Credit unions can select to have a new member temporary password be valid for one to seven days (seven being the default).</li> <li>The members will not be able to access their online account after a configured period (1 to 7 days with 7 being the maximum allowed).</li> </ul>	<p>Use <b>Tool #569 Online/Mobile/Text Banking VMS Config</b> to configure the number of days until this password is expired.</p> <p>To allow a member in after the period, the MSR must <u>reset</u> the password using <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update</b></p>

<i>Decision</i>	<i>Choices Offered by It's Me 247 / CU*BASE</i>	<i>For configuration...</i>
<b>Audio/Online Banking Access</b>		
Do you want to market an open enrollment period on a regular basis?	<ul style="list-style-type: none"> <li>Configure promotional campaign periodically to encourage members who are active but not allowed access due to an expired password, such as once or twice a year)</li> </ul>	Use <b>Tool #234 Config New Online User Promo Campaign</b>
<b>Maintenance Tasks</b>		
Do you want to allow your staff to set custom passwords for members who are having trouble setting their own?	<ul style="list-style-type: none"> <li>If not, you can choose to disable the custom password option for all memberships; MSRs must <u>reset</u> a password to the temporary password then instruct the member to change the password manually using <b>It's Me 247</b></li> <li>Develop an internal credit union policy and procedure for your staff</li> </ul>	Contact Client Services to disable the custom password option. Or grant access to <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b> only to staff that are authorized to set custom passwords
How will MSRs validate identity when a member calls to be reactivated after his/her password has expired?	<ul style="list-style-type: none"> <li>Develop an internal credit union policy and procedure for your staff</li> </ul>	To allow a member in after the expiration period, the MSR must <u>reset</u> the password using <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b>
What if a member loses his or her password?	<ul style="list-style-type: none"> <li>Develop an internal policy and procedure MSRs and phone staff should use to verify identity.</li> <li>Reset the password to the configured credit union temporary password; the member will be required to change it immediately upon logging in</li> </ul> <p><i>HINT: You may even want to set up a workstation in the lobby that members can use to change their password right away.</i></p>	Use <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b> to reset a password
What if a member knows his or her password but forgets the answers to his or her challenge questions?	<ul style="list-style-type: none"> <li>Develop an internal policy and procedure MSRs and phone staff should use to verify identity.</li> <li>Delete the member's challenge questions and answers in CU*BASE; the member will be required to select new questions and answers immediately upon logging in. NOTE: The credit union employee will see only the questions, not the answers</li> </ul> <p><i>HINT: You may even want to set up a workstation in the lobby that members can use to change their password right away.</i></p>	Use the <i>Online Banking</i> button in Inquiry or Phone Operator to delete the member's questions and answers. A confirmation will be required. (This only clears the answers.)
What if a member forgets his or her password and also forgets the answers to his or	<ul style="list-style-type: none"> <li>Develop an internal policy and procedure MSRs and phone staff should use to verify identity.</li> <li>Reset the password to the configured credit union temporary password; the member will</li> </ul>	Use <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b> to delete the member's questions and answers. A confirmation will



<i>Decision</i>	<i>Choices Offered by It's Me 247 / CU*BASE</i>	<i>For configuration...</i>
her challenge questions?	<p>be required to change it immediately upon logging in</p> <ul style="list-style-type: none"> <li>• Delete the member's challenge questions and answers in CU*BASE; the member will be required log in using the temporary password and to change his or her password and the answers to the challenge questions immediately upon logging in. NOTE: The credit union employee will see only the questions, not the answers</li> <li>• <i>HINT: You may even want to set up a workstation in the lobby that members can use to change their password right away.</i></li> </ul>	<p>be required. This process will also reset the member's password to the temporary password.</p>
What if a member forgets his or her username?	<ul style="list-style-type: none"> <li>• There is no "I forgot my username" feature in online banking. If members forget their username, they will need to contact the credit union for assistance, just as members do when they forget their account number.</li> <li>• Develop an internal policy and procedure MSRs and phone staff should use to verify identity.</li> <li>• Either view or delete the member's username. NOTE: The employee will see the member's username prior to deleting it.</li> <li>• Refer to Page 3 for rules when creating usernames.</li> </ul>	<p>Use <b>Tool #14 Member Personal Banker</b> or <b>Tool #72 Update Audio/Online Banking Access</b> to view or delete the member's username.</p> <p>A confirmation will be required if deleted. The member will then need to create a new username the next time he or she logs into online banking.</p>

# To ACTIVATE OR NOT TO ACTIVATE?

Another way to control access is to simply disable access for member accounts (either for all memberships or just new members) until a member actively requests access. **(Remember that you can also permanently disable any individual member's account so that access is never granted.)** Not only does this method allow you to monitor online banking enrollments, it also lets you work directly with a member to ensure they receive the proper training and an introduction to features such as product rates and opening accounts online. This is ideal for problem members, as well as for members that have specifically requested deactivation of the online banking channel.)

In addition, this method allows MSRs to verify a member's identity, and then require the member to change his or her password while still in the lobby, reducing the risk that someone will access their account using the system-assigned password before they do. While this method requires more staff time, it can be effective if your credit union can use the opportunity to cross sell your member on all of the benefits of your self-service products.

## ACTIVATE/DEACTIVATE VIA MEMBER PERSONAL BANKER

At any time, the credit union can select to activate or deactivate a member's access to online banking via the Audio Banking/Online Banking Access screen, accessed via **Tool #14 Member Personal Banker**, then *Online Banking/ARU (activate, change PIN/password; view password history)*. The top of the screen determines if the member will have access to online banking. (Left is for online banking, right is for Audio Banking as indicated by the mouse and phone icon. The MSR would simply uncheck the Online Banking checkbox to deactivate (or check to activate) and select a reason code.

### Activate or Deactivate

Session 0 CU\*BASE GOLD Edition - ABC TESTING CREDIT UNION

File Edit Tools Help

**Update Audio/Online Banking Access** UPDATE

Account **MARY MEMBER**

The Member is Allowed to Access This Account Using

<input checked="" type="checkbox"/> Online banking Reason D02	<input checked="" type="checkbox"/> Audio response Reason D02
---	---

**Change Password**  
☐ Reset password to the last four digits of the member's SSN & the member's

**Change PIN**  
☐ Reset PIN to last four digits of member's SSN

For example, if a credit union does not activate the member during membership enrollment, it can select to have their MSRs activate the member via this manner. Additionally, this screen can be used to deactivate a member, for example, to block access for a member by credit union policy or at the member's request. MSRs would simply check or uncheck the activation checkbox. (Unchecked meaning deactivated.)

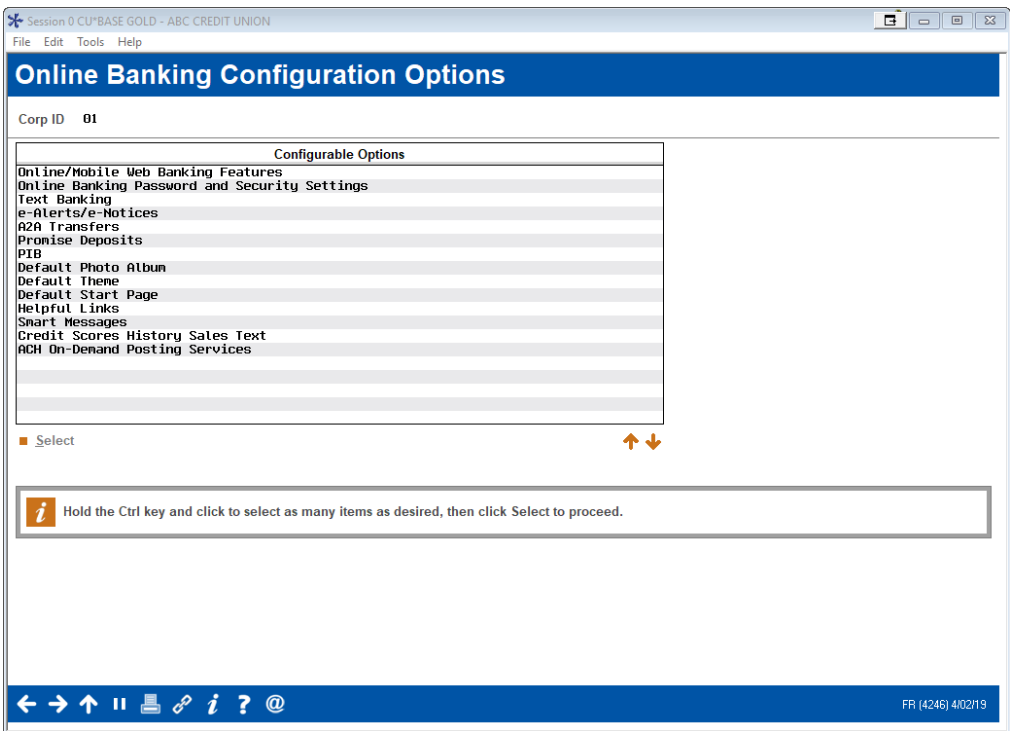
- NOTE: If a member is already on the fraud block list, you will receive the message, "SSN/TIN appears on block list" and will be unable to check the *Online Banking* box. Refer to page 11 for more information about fraud block lists.

# ONLINE/MOBILE PASSWORD AND SECURITY SETTINGS/MFA CONFIGURATION

Credit unions can set many of their online and mobile password settings themselves; however, they can also ask a Client Service Representative for assistance. Many of these settings have been covered previously in this booklet.

To access the Online/Mobile Password and Security Settings, use **Tool #569 Online/Mobile/Text Banking VMS Config**. From there select *Online Banking Password and Security Settings*.

## Online/Mobile/Text Banking VMS Config (Tool #569)



From here select *Online Banking Password and Security Settings*.

## Online Banking Password and Security Settings

Session 0 CU\*BASE GOLD - ABC CREDIT UNION  
File Edit Tools Help

**Online/Mobile Password and Security Settings** Corp ID 01

**Formula for Temporary Passwords**  
Use this formula for temporary passwords (password resets & new members via Method A): Temporary passwords expire after 24 hours  
Last 4 of SSN & birth year

New Members - Method A (Formula)	New Members and First-Time Users - Method B (Multi-factor)
<p>This method uses the temporary password formula for brand-new members using online/mobile banking for the very first time.</p> <p>With this method, existing members that are no longer within this time window must request a password reset or be included in a promotional campaign in order to log in for the first time.</p> <p># of days after membership open date a brand-new member has to log in for the first time before the temporary password expires 7 (1-7)</p>	<p>This method uses a multi-factor technique for brand-new members. This technique can also be used by existing members the very first time they access online/mobile banking.</p> <p>Allow first-time setup via Code sent via text or email (Note: Access codes will expire 24 hours after being requested by the member.)</p>

Other General Password Settings	Other Security Settings
<p># of password retries allowed before the account is locked 3 (Note: Member can still use the Forgot Password feature and answer their security questions.)</p> <p><input type="checkbox"/> Enforce complex password (will force password change unless password is already complex)</p> <p><input checked="" type="checkbox"/> Allow employees to manually enter a custom PIN or password for a member (Note: There is no expiration period for this password and the member will not be forced to change upon login.)</p> <p>Minimum length for password 06 (6-10) (Note: Maximum length is 256 characters)</p> <p>Expire stale passwords after 090 days of non-use (Max=90, Never expire=999)</p>	<p><input type="checkbox"/> Force member to set up a username for logging in (in place of their account #)</p>

Update

← → ↑ ↓ ⏸ ⏹ ⏶ ⏷ ⓘ ? @ (6819)

Here you can set online banking password configurations, including your temporary password configuration and minimum password length, without having to contact us to access the controls for you. See the following table for a more detailed discussion on the fields on this screen. As always, a Client Service Representative can assist you with understanding your options. Use Enter to access the screen below.

### Second Screen

Session 0 CU\*BASE GOLD - ABC TESTING CREDIT UNION  
File Edit Tools Help

**Online Banking Password and Security Settings** Corp ID 01

Require two factor authorization ☐ No ☐ Personal ☐ Business ☒ Both

**Standard Online Banking Member Login**

If two factor, use ☐ Code sent via text or email ☐ Code sent via email ☐ Code sent via text

Remember my device feature for desktop/mobile web:  
Expire device registration after 30 days (0=Expire after every login, 1-998=actual # of days, 999=never expire)

Remember my device feature for mobile app:  
Expire device registration after 30 days (0=Expire after every login, 1-998=actual # of days, 999=never expire)

**Business Banking Multi-Login**

Remember my device feature for desktop/mobile web:  
Expire device registration after 999 days (0=Expire after every login, 1-998=actual # of days, 999=never expire)

Remember my device feature for mobile app:  
Expire device registration after 999 days (0=Expire after every login, 1-998=actual # of days, 999=never expire)

Update

← → ↑ ↓ ⏸ ⏹ ⏶ ⏷ ⓘ ? @ FR UCUBSEC:02 3/13/24

The MFA activation and number of days before device registration expiration is configured on this second screen. On this screen, select whether the one-time login passcode will be sent to the member's email, phone, or both. Then designate the number of days the device registration will be active on the member's device before they will need to register via MFA again (999 is never expire). Use Update (F5) to save the changes. When ready, return to this screen to activate this feature. See the following table for more details.

Different settings can also be set for **BizLink 247** business online banking at the bottom of the screen.

## CONFIGURATION OPTIONS FOR FIRST TIME USER MFA AND SECURITY SETTINGS

Following are the things that can be configured on these the two screens shown previously.

<i>Field Name</i>	<i>Description</i>
<b>Formula for Temporary Passwords</b>	
Use this formula for temporary passwords (password resets & new members via Method A)	<p>This setting controls what the members temporary online banking password will be set to. Members receive temporary passwords for a controlled length of time (24 hours) in certain situations, such as password reset, promotional campaign and when activated as a new member. Credit unions have four options for this configuration:</p> <ul style="list-style-type: none"> <li>• Birth year + First 2 Letters of Last Name (ALL CAPS) (X)</li> <li>• Last four of SSN + Birth year (N)</li> <li>• Last four of SSN (default) (S))</li> <li>• First 4 of SSN and First 2 Letters of Last Name (ALL CAPS) (B)</li> </ul> <p>(Corporations will use their TIN, origination date, and company name (in place of last name.)</p> <p>When a credit union employee resets a member's password, the reset screen will clearly state this selection so that the employee can advise the member correctly.</p>
<b>New Members – Method A</b>	
First time login – Method A	Method A uses the temporary password and their account number to log into online banking. See also Method B below.
# of days a new member has to log into online banking (1-7)	The default for this setting is seven. If a credit union activates a member in online banking during the creation of their membership and during workflow controls, this setting limits the number of days that member can log into online banking. Credit unions can select from one to seven days. After this configured number of days, the member must call the credit union to reset his or her password.
<b>New Members - Method B</b>	
Method B: Allow first time setup via email and/or text message	This method uses a multi-factor authentication (MNA) technique for brand new members. This technique can also be used by existing members the very first time they access online/mobile banking. To use this method, select which delivery method you would like members to use, email and/or text. The member will then access online banking and select a link labeled, "First Time User?" The member then chooses the delivery method they prefer, based on what has been activated by the credit union, and what information is on file for the membership.

Field Name	Description
	<p>This will prompt the activation code to be sent to the member, which is then entered on the following screen prompt. The code is good for 24 hours after initial request, after which the member must request a new code.</p> <p>See also more on multi-factor authentication (MFA) on page 24. This section includes pictures of the member experience.</p>
<b>Other General Password Settings</b>	
# of password retries allowed before the account is locked	<p>This is informational only and cannot be changed. The member has three attempts to enter his or her password correctly. If a member enters three incorrect password, online access to the membership is not allowed.</p> <p>If a PIN/password is disabled due to invalid tries, an employee can use <b>Tool #14 Member Personal Banker</b> to reset the password OR the member can use the forgot password feature and answer their security questions to reset their password.</p>
Enforce complex password (will force password change unless password is already complex)	<p>You can elect to force members to follow complex password rules when setting up their online banking password. This requires a combination of three of the following to be included in the password: lowercase letter, uppercase letter, number, and special character.</p> <p>Leave the box unchecked if you do not wish to enforce these rules. (Members can still use this format if they wish, of course, but will not be forced to do so.)</p> <ul style="list-style-type: none"> <li>NOTE: Activating this will force members to change their current passwords immediately (if they do not already have a complex password).</li> </ul>
Allow employee to manually enter a custom PIN for the member	<p>Check this box if you want credit union MSRs and other staff to be able to enter a member's password using <b>Tool #14 Member Personal Banker</b>. This would allow a member who is having trouble setting his password online to ask a staff member to enter his preferred password for him.</p> <p>Leave the box unchecked to block this feature. Instead, staff would need to reset the PIN to the selected temporary password setting (see above), which would then force the member to change his password the next time he logs on to online banking.</p> <ul style="list-style-type: none"> <li>NOTE: There is no expiration for this password and the member will not be forced to change upon login.</li> </ul>
Minimum length for password (6-10) (Note: Maximum length is 256 characters.)	<p>Use this field to specify the minimum number of characters that must be used for a member's online banking password. The maximum length is 265 characters. This length must be at least 6 characters long, with a maximum of ten characters. In general, the longer and more complex a password is, the more difficult it is for an unauthorized person to obtain it.</p> <ul style="list-style-type: none"> <li>NOTE: If you increase your minimum length, all members with a password length shorter than the new minimum length will be required to change their password the next time they log in.</li> </ul>
Expire stale password after xx days of non-use (max = 90, Never expire 999)	<p>You may use this field to activate an "expiration" period for online banking members. Enter the number of days for the expiration period – maximum 90 days. Enter 999 in this field to select to never have passwords expire.</p>

Field Name	Description
	<p>“Expiration” does not mean the password itself needs to be changed periodically; this expiration comes into play only after a member has not logged into online banking for a certain period.</p> <p>The expiration feature provides an extra measure of security for dormant memberships or members who do not choose to use your self-service options. (Remember that you can also choose to deactivate an individual member's access to these systems completely using <b>Tool #14 Member Personal Banker</b>.)</p> <p>When a member attempts to access his or her account through online banking but has not done so for more than the specified period of days, he or she will be instructed to contact the credit union to reactivate the password. (If the member's password does expire, this member can also always use the “I forgot my password feature and answer a security question to reset the password.”)</p>
<b>Other Security Features</b>	
Force usernames	<p>Check this box to force members to create usernames in online banking and use them in place of their account number when logging into standard and mobile web banking.</p> <p>Otherwise, usernames are an optional security feature.</p>

## CONFIGURATION OPTIONS FOR STANDARD LOGIN MFA

Below are the configuration options for the second MFA login screen.

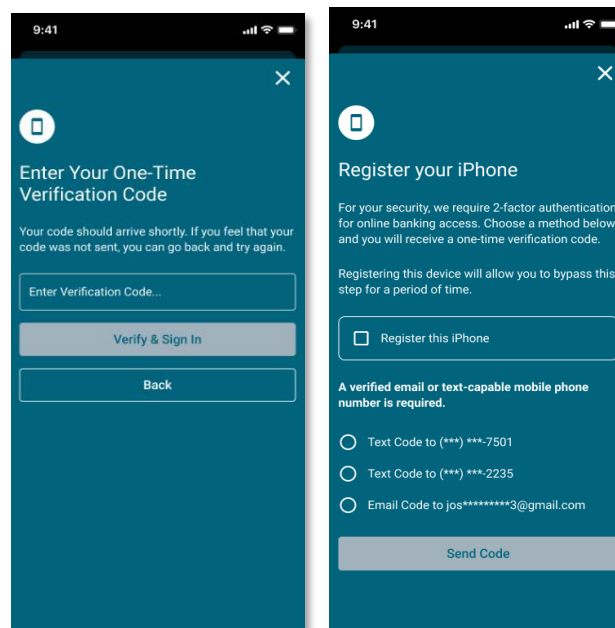
Field Name	Description
<b>Activation</b>	
Require two factor authentication	To activate the feature for <b>It's Me 247</b> , select Personal.
<b>Standard Online Banking Member Login</b>	
If two-factor, use	Select whether the code should be sent via email, text message, or both. This determines what will be presented to the member in online banking. <i>Refer to the following frequently asked questions in the section below for more details.</i>
Remember my device feature for desktop/mobile web	Set the number of days a device will be remembered after MFA registration for the desktop/mobile web environment. MFA will not be required for this device in the desktop/mobile web environment until the configured number of days has passed. <i>Refer to the following frequently asked question in the section below for more details.</i>
Remember my device feature for mobile app	Set the number of days a device will be remembered after MFA registration for the mobile app environment. MFA will not be required for this device in the mobile app until the configured number of days has passed. <i>Refer to the following frequently asked question in the section below for more details.</i>
<b>Business Banking Multi-Login</b>	
Remember my device feature for desktop/mobile web	Set the number of days a device will be remembered after MFA registration for the desktop/mobile web environment. MFA will not be required for this device in the desktop/mobile web environment until the configured number of days has passed. <i>Refer to the following frequently asked question in the section below for more details.</i>

Field Name	Description
Remember my device feature for mobile app	Set the number of days a device will be remembered after MFA registration for the mobile app environment. MFA will not be required for this device in the mobile app until the configured number of days has passed. <i>Refer to the following frequently asked question in the section below for more details.</i>

## MFA ONE-TIME PASSCODE AND REGISTRATION AT ONLINE BANKING LOGIN

Require that the member request a code for authentication to online banking; these are also referred to as “one-time passcodes” or two-factor authentication. Members can opt to register their device so that authorization isn’t required each time they log in (see the MFA FAQ below for more details!)

- Concerned about your members having to use MFA frequently? *Configure a set number of days for the device to be remembered.*
- Concerned your phone database and personal details are not up to date in CU\*BASE? *Encourage your members to update their phone number using an online banner, form, or Xtend campaign.*
- Interested in having different controls for business banking, standard browser banking, and mobile app? *Set different controls for each in the configuration screen.*



This feature is configured on the second security setting configuration screen discussed in the previous section.

### MFA One-Time Passcode at Login and Device Registration Frequently Asked Questions (FAQ)

Learn more about one-time passcode MFA at login in the knowledge base:

1. [After my credit union activates \*\*It's Me 247\*\* multi-factor authentication \(MFA\), will my members who use their MACO credentials \(voice, fingerprint, photo ID, or custom PIN\) with the mobile app also be required to use a one-time passcode to register with device registration?](#)



2. [I see there are “mobile phone” and “can send text messages to this number” checkboxes on the phone database screen in CU\\*BASE. Do either of these need to be checked in CU\\*BASE for that phone number to be used for multi-factor authentication \(MFA\)?](#)
3. [My member has four phone numbers associated with their membership. Can they use any of these numbers for multi-factor authentication \(MFA\) for \*\*It's Me 247\*\*?](#)
4. [Can I set different expiration days for the device registration for multi-factor authentication \(MFA\) for members using a browser versus mobile app banking to access \*\*It's Me 247\*\*?](#)
5. [Does online membership opening process \(MOP\) support multi-factor authentication \(MFA\)? How does that process work?](#)
6. [With multi-factor authentication \(MFA\), what situations would cause a member who had already registered their device with a one-time passcode to need to register it again?](#)
7. [I hear that when it is implemented, multi-factor authentication \(MFA\) will only work with members who authenticate using the aggregator Plaid. What can I do about other aggregators my members have given their login credentials to?](#)
8. [What are some strategies I can use to clean up my phone database for my multi-factor authentication \(MFA\) rollout?](#)
9. [Does Xtend offer a data hygiene campaign to assist me with cleaning up my email and phone numbers for my MFA rollout?](#)
10. [What considerations should I have about Money Map and multi-factor authentication \(MFA\)?](#)
11. [What phone numbers are presented to the member for the one-time passcode for multi-factor authentication \(MFA\) for “It's Me 247”?](#)
12. [I see you can set online banking MFA \(multi-factor authentication\) to require device registration after a set number of days. What happens if my credit union changes this number of days in the CU\\*BASE configuration?](#)
13. [My credit union is activating multi-factor authentication \(MFA\) during online banking login. Can we now discontinue members having to answer their security questions?](#)
14. [After my credit union activates multi-factor authentication for \*\*It's Me 247\*\*, do my members using the “jump” feature \(to access a second membership without entering credentials\) need to use MFA during this jump?](#)
15. [My credit union has activated multi-factor authentication \(MFA\) for personal information changes in \*\*It's Me 247\*\*. How does the member experience for MFA during login differ?](#)

16. [Could "Incognito Mode" impact Multi-Factor Authentication \(MFA\) functionality?](#)
17. [How do I control the costs I incur with multi-factor authentication \(MFA\) text messages?](#)
18. [Are there costs associated with offering multi-factor authentication \(MFA\) via online banking?](#)

## MFA FOR NEW MEMBERSHIPS

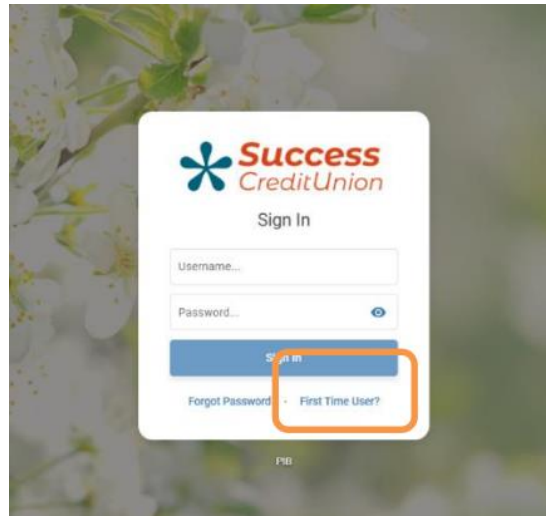
For new member enrollment, your credit union can elect to ask that members authenticate by entering a code that is texted or emailed to them.

This MFA feature for new memberships is available as one option for first time login. It is activated in the *Online/Mobile Password and Security Settings* screen. See the section starting on page 19. The MFA authentication method is called *Method B*, covered on page 21.

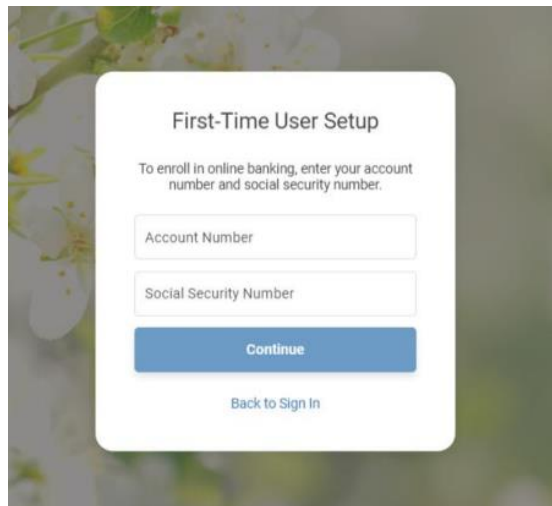
Once this feature is activated, the member will experience a different first-time enrollment flow. Instead of entering in the temporary password (Method A), they will be required the code. The email or phone number that the code is sent to must be associated with the membership in CU\*BASE. The code is active for 24 hours.

*See following screenshots for more details.*

First the member will click **First Time User**.



Then the member will complete the fields, entering in their account number and social security number. The member will then click **Continue**.



First-Time User Setup

To enroll in online banking, enter your account number and social security number.

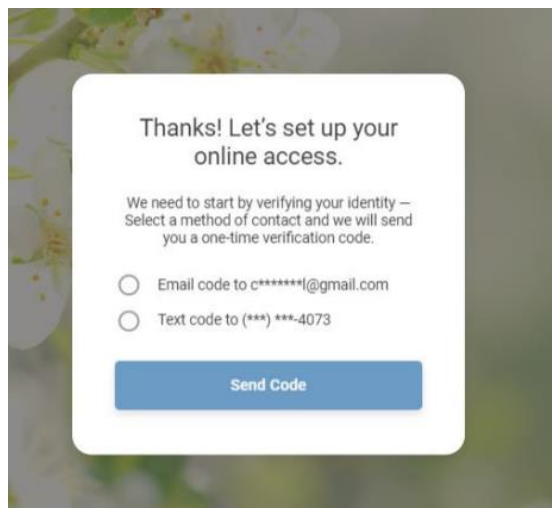
Account Number

Social Security Number

Continue

[Back to Sign In](#)

The email and phone numbers presented are already associated with the membership. The member selects where they would like to receive the code and clicks **Send Code**.



Thanks! Let's set up your online access.

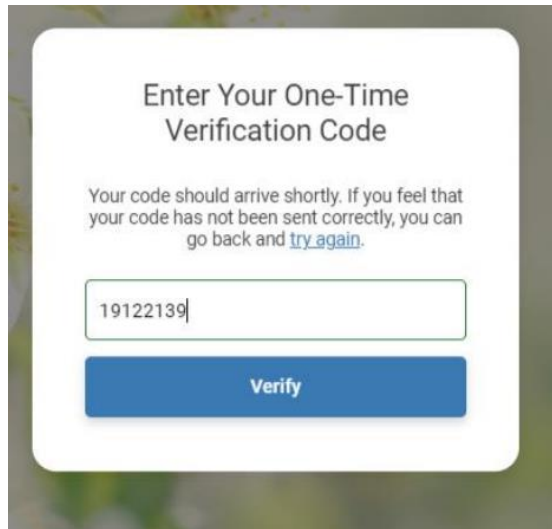
We need to start by verifying your identity — Select a method of contact and we will send you a one-time verification code.

☐ Email code to c\*\*\*\*\*l@gmail.com

☐ Text code to (\*\*\*) \*\*\*-4073

Send Code

The member enters the code and clicks **Verify**.



Enter Your One-Time Verification Code

Your code should arrive shortly. If you feel that your code has not been sent correctly, you can go back and [try again](#).

19122139|

Verify

Next the member sets up their password, username, security questions, etc. as with any first-time login to online banking.

## MFA FOR PAY ANYONE OR PERSONAL INFORMATION UPDATE

Your credit union can also optionally activate MFA to provide even greater security (beyond the initial online banking login) for two member-facing activities (Pay Anyone and personal information updates).

To activate MFA for either of these features, use CU\*BASE **Tool #569 Online/Mobile/Text Banking VMS Configuration** and then *Update Online Banking Security Settings* to access the screen shown below.

- **For MFA for personal information changes**, check *Direct update with two factor (text/email)* for *Allow main of personal info by member (online)*.
  - If you activate this feature for personal information changes, you cannot set the member's changes for review by your credit union. All changes are implemented immediately.
- **For P2P (Pay Anyone)** check *Apply two factor authentication to P2P*.
  - This provides MFA to the Pay Anyone module which provides access to enrollment, sending of payments, and unenrollment.
  - NOTE: MFA is not supported by the Pay Anyone micro-app. Learn more about the micro app: <https://store.cuanswers.com/product/pay-anyone/>.

### "Update Online Banking Security Settings" Accessed from Tool #569

Use this option to allow direct update of personal information via two-factor authentication.

Use this option to required MFA for P2P transfers.

Session 0 - ABC TESTING CREDIT UNION

File Edit Tools Help

### Update Credit Union Online Banking Settings

CHANGE

Corp ID 01

☒ Allow new membership application online Member Instructions

☒ Apply membership application fee

Dividend application to be used SH

☒ Activate savings rate board Member Instructions

☒ Activate certificate rate board Member Instructions

☒ Activate loan rate board Member Instructions

☐ Require co-applicant if marital status is Married

Allow maint of personal info by member (online) ☐ Direct update (no approval) ☐ Reviewed update (approval required) ☐ No

☒ Direct update with two factor (text/email)

☒ Allow member to enter account nicknames

Default setting when setting up transfer control list ☒ All sub-accounts ☐ Owned sub-accounts only ☐ Specify Member Instructions

☒ Allow member to change Reg E Opt In/Out choice

☒ Show who was served (either a jump guest or via Teller Currently Serving) in transaction history

☒ Apply two factor authentication to P2P

Email address to notify of incoming request

(Includes only personal info and contact requests. Other notifications are configured separately.)

Update

Instructions

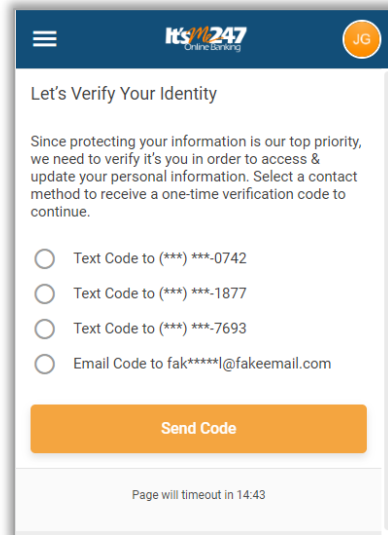
← → ↑ || ⏏ ⓘ ? @

FR 14238 10/03/24

[Refer to this help topic for more details.](#)

Once either feature on the previous page is activated, the first MFA pop up window allows the member to indicate whether they want to receive the MFA code via email or text message. The phone numbers and emails presented are configured on the member's membership in CU\*BASE.

### First MFA Pop Up Window

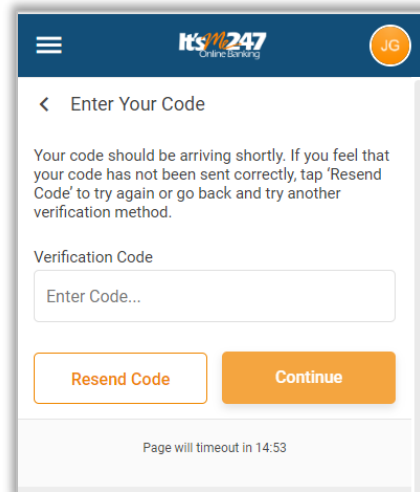
A screenshot of the 'First MFA Pop Up Window' from the 'It's Me 247' mobile app. The header shows a hamburger menu, the 'It's Me 247' logo, and a user icon 'JG'. The title is 'Let's Verify Your Identity'. The text explains that protection is a priority and a one-time verification code will be sent. There are four radio button options: 'Text Code to (\*\*\*-0742)', 'Text Code to (\*\*\*-1877)', 'Text Code to (\*\*\*-7693)', and 'Email Code to fak\*\*\*\*\*@fakeemail.com'. An orange 'Send Code' button is at the bottom. A footer note says 'Page will timeout in 14:43'.

The member clicks *Send Code* to receive the code.

- NOTE: The MFA code expires after 15 minutes.

The member then advances to the second pop up window and enters the MFA code in the space provided.

### Second MFA Pop Up Window

A screenshot of the 'Second MFA Pop Up Window' from the 'It's Me 247' mobile app. The header is the same as the first window. The title is '< Enter Your Code'. The text says 'Your code should be arriving shortly. If you feel that your code has not been sent correctly, tap 'Resend Code' to try again or go back and try another verification method.' There is a text input field labeled 'Verification Code' with the placeholder 'Enter Code...'. Below the field are two orange buttons: 'Resend Code' and 'Continue'. A footer note says 'Page will timeout in 14:53'.

The member then clicks *Continue* to proceed to access the protected feature.

- This access is granted for the entire online banking session. The member does not need to enter a new code until they log off **It's Me 247**. Then, a new code is required the next time they want to access the Pay Anyone module.

---

# **“TRY IT BEFORE YOU BUY IT!” –**

## **PROMOTIONAL CAMPAIGNS**

Want to increase the number of members using **It's Me 247**? Encourage more people to use online banking through the use of a promotional campaign. You can, for example, select January 2014 as your promotional period. During this month, you can allow members who do not have access to online banking (with for example, an expired password due to non-use or a temporary password past its reset time window) access to online banking – for a “try it out” period. This allows you *sell* online banking services as a special value your members receive from belonging to the credit union. You can even send these members targeted marketing to encourage them to sign on and become new online banking users. And it requires very little time on the part of your staff—members can log in any time during the promotional period that is convenient for them.

These members would otherwise have to call your credit union to get access.

Your marketing team can handle promotional campaigns on their own and configure their own program via **Tool #234 Config New Online User Promo Campaign**. From the promotional software, they can select which members they want to include in the promo (exclude, for example, members without an email address) and view a listing of these members to monitor progress with the program. CU\*BASE even allows the printing of reports and creation of a Member Connect database file for targeted email campaigns.

- Only members who are activated for online banking are included in promotional campaigns. If your credit union does not activate members (when they open a membership), these (non-activated) members will not be included in the promotional campaign.

Once the period has expired, any members who have not logged in at least once during the promotional campaign period will automatically be instructed to contact the credit union for activation the next time they attempt to log in.

### **Who Qualifies for a Promotional Campaign?**

Below are the members who are by default allowed in a promotional campaign:

- Members who are activated to use Online Banking, members who are not activated will not be included.
- Members who have entered their password incorrectly three times
- Members whose password has expired (they have not logged in for the number of days until a password expires)
- Members who just joined the credit union and missed the configured range for new members to log in
- Members who had their password reset by an MSR and missed the window to log in
- Members who entered an invalid security question three times

The promotional campaign software allows you to select to exclude some of these members based on the following criteria:

- Members who do not have email addresses

- Members who have never logged in or have not logged in since a certain period of time.

## PROMOTIONAL CAMPAIGN CONFIGURATION

### Config New Online User Promo Campaign (Tool #234)

The entry screen allows you to name your promotional campaign and set the date range of the campaign. Once you press Enter, the end date will be calculated.

### Promotional Campaign (Date Selected)

Then use *Actv/View Mbrs* (F10) to select the members who will be included in the campaign.

## Promotional Campaign (Member Selection)

These filters allow you to exclude members who might otherwise qualify. See bulleted list below for exclusions.

Session 0 CU\*BASE GOLD Edition - CU\*ANSWERS TEST CREDIT UNION (CU)

File Edit Tools Help

### Members Affected by Promotional Period

☐ Limit list to only members with an email address  
☒ Include both members with and without an email address

☐ Limit the list to members who have logged on at least once  
 And who have logged in since  [MMDDYYYY]

☐ Limit the list to members who have never logged in

**i** Determine which members are affected by using the filters to the left, then either press Enter or click the Refresh button below.

Account	Name	Last Logged In	Last Opened	Use Agreement	Has Email	Has User Name
9	OLETON	Oct 27, 2011	Sep 25, 2008	Feb 24, 2010	Y	N
8	PS	Nov 14, 2011	Jul 01, 1987	Jun 17, 2010	N	N
4	LAND	Feb 23, 2009	Jul 01, 1987	0/00/0000	N	N
2	LAND	Jul 23, 2012	Jul 25, 2008	Jul 19, 2010	N	N
3	CFARLAND	Feb 24, 2011	Jul 25, 2008	Jul 19, 2010	N	N
4	RLAND	Feb 24, 2011	Feb 24, 2011	0/00/0000	N	N
8	SNER	0/00/0000	Jul 01, 1987	0/00/0000	N	N
2	NIX	0/00/0000	Jul 01, 1987	0/00/0000	N	N
0	3	0/00/0000	Jul 01, 1987	0/00/0000	Y	N
1	ATION	Jun 26, 2012	May 16, 1995	Mar 05, 2010	N	N
2	TERNATIONA ASSOC	Feb 20, 2009	May 16, 1995	Jan 16, 2009	N	N
8		Jan 02, 2007	May 17, 1995	Mar 06, 2003	N	N
1	ELL	Oct 02, 2012	May 18, 1995	Feb 15, 2010	N	N
2	SSIG	Nov 13, 2012	May 18, 1995	Feb 15, 2010	N	N
4		Jun 15, 2007	May 19, 1995	Jun 15, 2007	N	N
5	HA	Nov 14, 2011	May 19, 1995	Feb 16, 2010	N	N

↑ ↓

Total number of members affected by promotional period 23,271

**i** Members blocked from Online Banking are not included in the campaign.

BT (3659) 7/18/13

This screen allows you to filter to exclude:

- Members without an email address (defaults to include members with and without one)
- Member who have either never logged in or who have not logged in since a certain date (defaults to include both members who have logged in and never logged in)

Use *Refresh* or press Enter to refresh your list to exclude (or include) members based on these selections.

This screen includes the last log in date, membership open date, the date the member accepted the Online Banking Use Agreement, whether the member has an email account and whether the member has a username for online banking access.

To create a file for Member Connect use *Print* (F14) to view the screen below. Check the Export to file checkbox and enter the file name. Then press Enter to generate the file.

- NOTE: During a campaign, you can return to this screen to print updated results to a file for further analysis in Report Builder.



## Print a Member File

The screenshot shows a window titled "Session 0 CU\*BASE GOLD Edition - CU\*ANSWERS TEST CREDIT UNION (CU)". The window has a menu bar with "File", "Edit", "Tools", and "Help". Below the menu bar is a blue header bar with the text "List Members in an Online Banking Promotional Campaign". Underneath the header bar is a "Report Options" section with a "Response" column. In the "Report Options" section, there is a checkbox labeled "Export to file (optional)" and a text field labeled "File name" with the text "(optional)" next to it. To the right of the "Report Options" section is a "Job queue" section with a checked checkbox labeled "Job queue", a "Copies" field with the value "1", and a "Printer" field with the value "P1". Below the "Report Options" and "Job queue" sections is a large empty white area. At the bottom of the window is a blue bar with a row of icons: a left arrow, a right arrow, an up arrow, a pause icon, a print icon, a link icon, an information icon, a question mark icon, and an at-sign icon. In the bottom right corner of the blue bar, the text "BT (3843) 7/18/13" is displayed.

To activate the promotional campaign, use *Activate* (F10). Then use *Add/Update* (F5) to complete the activation.

## Confirmation of Activation

The screenshot shows a window titled "Session 0 CU\*BASE GOLD Edition - Confirm". The window has a menu bar with "File", "Edit", "Tools", and "Help". Below the menu bar is a white area with the text "This will update all 23271 members." and "Press Cnd/5 to Continue." Below the text is a blue bar with two buttons: "Add/Update" and "Skip". At the bottom of the window is a blue bar with a row of icons: a left arrow, a right arrow, an up arrow, a pause icon, a print icon, a link icon, an information icon, a question mark icon, and an at-sign icon. In the bottom right corner of the blue bar, the text "BT (32)" is displayed.

You will then return to the original screen where you can see the date the promotional campaign will begin. Once the campaign is activated, use *Actv/View Mbrs* (F10) to view the members in the campaign.

**List of Members During Campaign**

Here you can see that one member in the promotional campaign group has logged into online banking.

Session 0 CU\*BASE GOLD Edition - ABC TESTING CREDIT UNION

File Edit Tools Help

Members Affected by Promotional Period

Limit list to only members with an email address

Include both members with and without an email address

Limit the list to members who have logged on at least once

Limit the list to members who have never logged in

Include both members who have logged in and members who have never logged in

Account	Name	Last Logged In	Date Opened	Use Agreement	Has Email	Has User Name	Promotional Campaign Results
2 H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
5 W		Feb 14, 2013	Dec 12, 1964	Mar 12, 2010	Y	N	
7 H		0/00/0000	Dec 14, 1964	0/00/0000	N	N	
0 H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
1 W		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
0 J		Dec 31, 2011	Dec 12, 1964	Nov 08, 2010	Y	N	
7 C		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
1 H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
2 H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
5 N		Jun 08, 2011	Dec 12, 1964	Jun 08, 2011	N	N	
6 C		May 10, 2010	Dec 12, 1964	Oct 25, 2002	N	N	
8 W		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
1 C		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
2 C		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
9 F		Jul 05, 2006	Dec 12, 1964	Jul 05, 2006	N	N	
9 W		0/00/0000	Dec 12, 1964	0/00/0000	N	N	

Select

Total number of members affected by promotional period27,390

Total number of members who have logged in during promotional period1

Members blocked from Online Banking are not included in the campaign.

Print

Navigation icons

FR (3853) 7/18/13

On this screen, you can then see the progress of your campaign, by individual member (last column), as well as with a promotional campaign total at the bottom of the screen.

# MESSAGING ON ENTRY EXPLAINS REASON MEMBER NEEDS RESET

When members call because they cannot access online banking, your MSRs will immediately know the reason for the denial of access! After selecting to enter Member Personal Banker, the MSR will see a pop-up window explaining the reason for the lack of access. From this pop up the MSR can reset the password, without even entering the Update Audio/Online Banking Access screen of the member.

In order to view these messaging windows, you will need to first take the following steps:

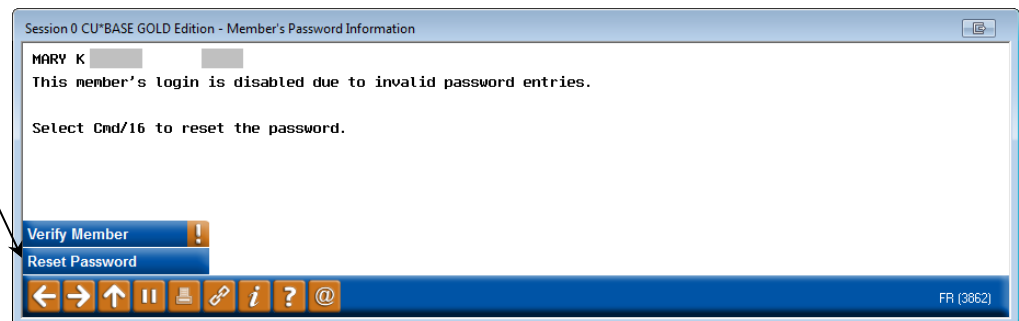
1. Select **Tool #14 Member Personal Banker**.
2. Enter the members account number and press Enter
3. Select *Online banking/ARU (activate, change, PIN/Password; view password history* and press Enter.

These screens will appear even before you access the Update Audio/Online Banking Access screen (shown on page 36)

## INCORRECT PASSWORD ENTRIES RESET

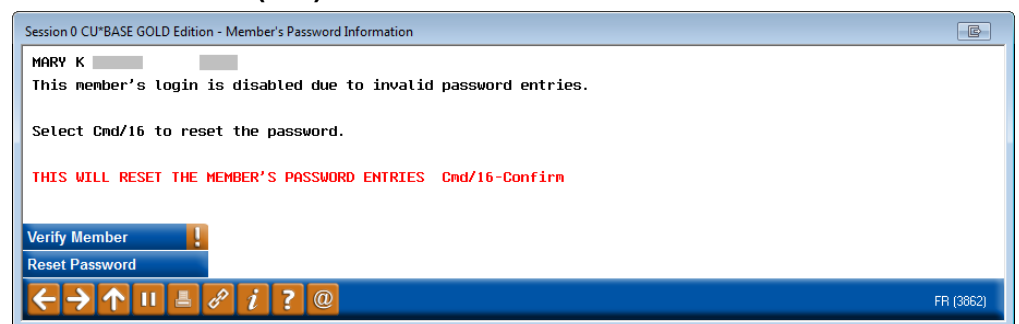
Members are locked out of their accounts after three incorrect password attempts. Following are the screens the MSR will see when assisting a member. After following the steps above, these three screens will walk the MSR through the password reset.

### Explanation that Password Needs Reset Due to Invalid Password Tries



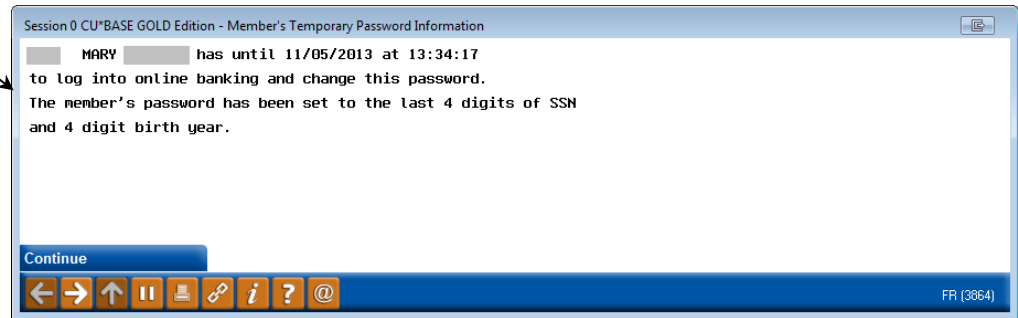
All entry explanatory screens have a *Verify Member* (F1) that MSRs can use to confirm the member's identity prior to assisting the member. This function key accesses the Verify Member screen which contains information such as the member's code word and birth date.

### "Reset Password" (F16) Selected



### “Reset Password” (F16) Selected

All confirmation screens clearly list the credit union's temporary password reset configuration selection, in this case the 4 digit birth year and first letters of last name (all caps). They also tell the MSR when this password will expire.



After pressing Enter the MSR will finally access the Update Audio/Online Banking Access screen. They may simply need to exit this screen.

### Update Audio/Online Banking Access Screen



This screen now clearly differentiates the online banking side and the audio banking side. If needed and allowed by the credit union, the MSR could assist the member further by assigning a custom online banking password.

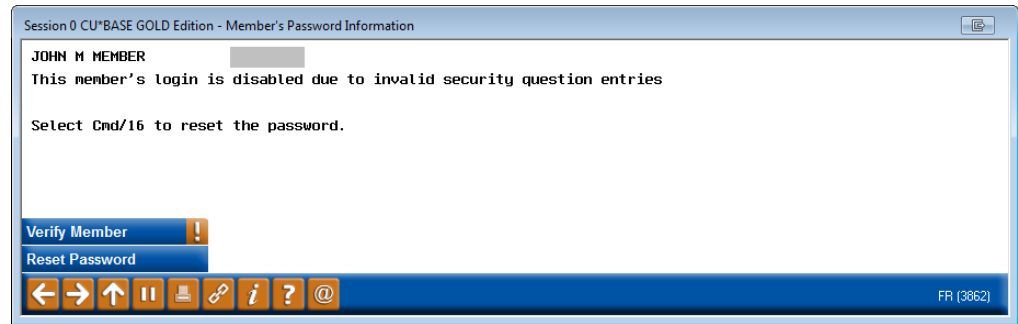
## RESET FOR THREE INCORRECT SECURITY QUESTION ANSWERS

A member may forget the answers to all of their security questions and may enter an incorrect answer three times. This locks them from their account and they will need to contact the credit union. Following are the screens your MSR will see when assisting this member.

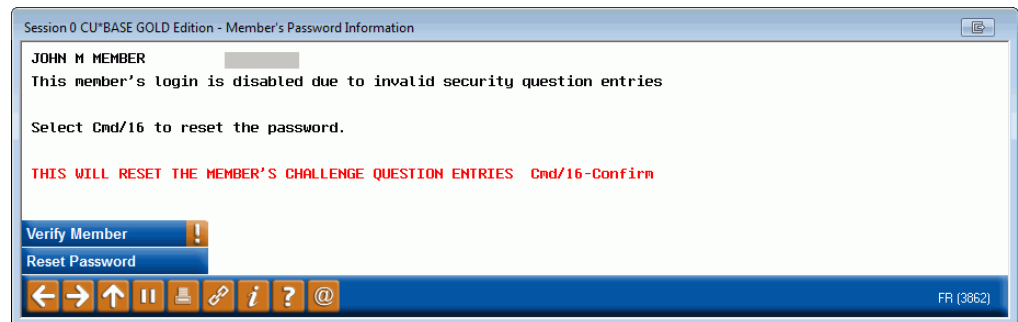
This process clears the answers of the security questions and also resets the member's password to the temporary password. Once reset, the member will have 24 hours to log in using the temporary password (according to temporary password rules). Once logged in the member will be required to

both select another password and also to select new answers to his or her security questions.

### Explanation that Access is Denied Due to Invalid Security Question Answers

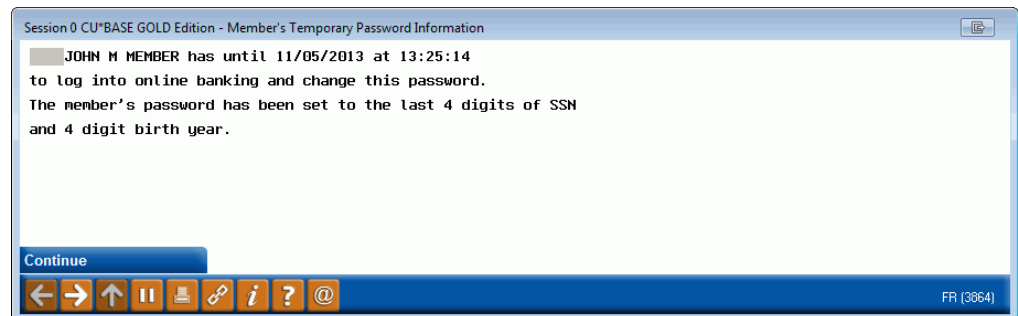


### "Reset" (F16) Selected



At this point the screen clearly explains how to clear the security questions.

### Reset Button Selected



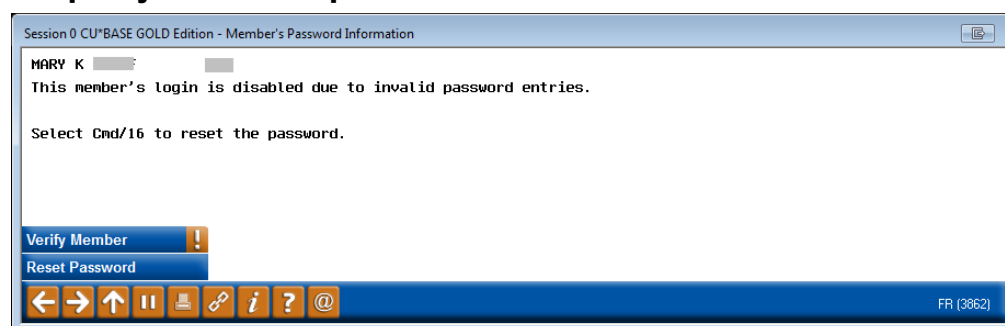
This screen clearly explains that the password has also been reset to the temporary password.

After pressing Enter the MSR will finally access the updated Update Audio/Online Banking Access screen. They may simply need to exit this screen (shown on page 36).

### Reset Expired Temporary Password

When a member receives a temporary password in this manner (password reset), the temporary password is valid for only 24 hours, as stated on the confirmation screen. If the member fails to log in during this period, the member will need to contact the credit union for another password reset. Following is the explanatory message screen the MSR will see when assisting this member:

## Temporary Password Expired

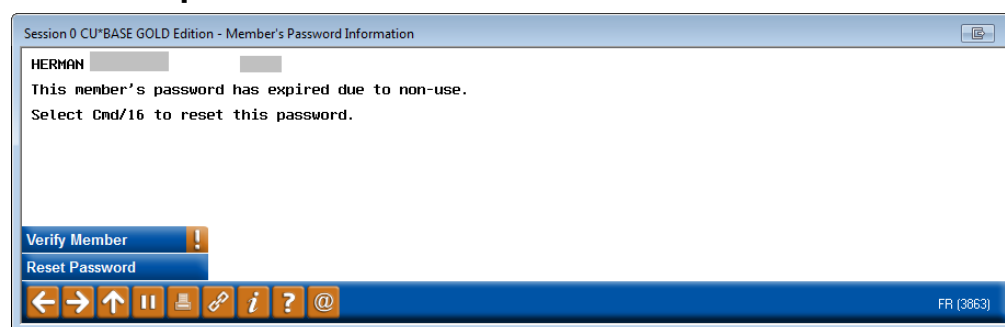


The other screens the MSR will see when assisting this member are similar to the ones the MSR sees when assisting a member who has entered their password incorrectly.

## RESET PASSWORD EXPIRED DUE TO NON-USE

In the *Online/Mobile Password and Security Settings* (covered on page 19), there is a setting for expired password days (maximum 90 days). If a member fails to log into online banking for a length of time greater than this range, the member's password will expire due to non-use. Following is the explanatory screen the MSR will see when assisting this member:

### Password Expired Due to Non Use



The other screens the MSR will see when assisting this member are similar to the ones the MSR sees when assisting a member who has entered their password incorrectly.

---

# USERNAMES

Members have the option of creating a username in the Info Center section of **It's Me 247**. (They can also add a username in mobile web banking.) They then use this username in place of their account number when they log into online banking. **Refer to Page 3 for rules when creating usernames.**

Your credit union can also set your *Online/Mobile Password and Security Settings* to require usernames (See page 19 for this configuration setting.) In this case, all members must create a username. **See Page 40 for more information.**

Remember that usernames are not passwords. They're intended to help keep the account number more private. But if the member forgets their username, they'll need to contact your credit union, the same as if they forget their account number.

Once the member has set up a username, they can change at any time in either standard or mobile web banking. However, once they have a username, they can't clear it. CU\*BASE does have a feature that allows a credit union employee to clear a username. In this case, the member is prompted to set up a new one the next time they login. See Page 41.

Usernames can be a maximum of twenty characters.

## OPTIONAL USERNAME

If your credit union does not require usernames, a member can create an *optional username* while in **It's Me 247**. The member can access the Username page via Info Center, then My Username. The member enters the username and then clicks the *Change My Username* button.

## Member Updates their Username

Change Username

Usernames are NOT case sensitive, must be 1–20 characters long, and must pass the following rules:

- Cannot contain any special characters
- Cannot begin or end with a space
- Cannot contain your account number
- Cannot contain your first or last name
- Cannot be all numbers

Current Username:

New Username

New Username

Change Username

Page will timeout in 14:07

Success Credit Union

This site contains links to other sites on the internet. We, and your credit union, cannot be responsible for the

Then at any time, the member can return to this screen to change their username in the Personal Info & Settings section.

## REQUIRED USERNAMES

Your credit union can elect to require that all members create a username.

- First and foremost, this feature **is optional** and must be activated by your credit union. You decide if and when you want to flip the switch.

To change your settings, you will need to fill out an “**It’s Me 247** Configuration Change Request form,” available under “I” on the CU\*BASE Reference page. [http://www.cuanswers.com/client\\_reference.php#1](http://www.cuanswers.com/client_reference.php#1). Contact Client Services for assistance.

### What happens once you activate required usernames?

- Members who already have a username won’t need to do anything.
- Existing members without usernames will login with their account number the next time they log into online banking. They will then automatically advance to the username setup screen and will be



prompted to create one. (See following image). They cannot advance until they create a username.

- Brand new members will log on with their account number. They will be asked to set up a username after accepting the Online Use Agreement (and before they set their password and challenge question answers).

#### **Member is Prompted to Enter Required Username**

Create a Username

Create a username for your OnlineBanking. Usernames are NOT case sensitive, must be 1-20 characters long, and must pass the following rules:

- Cannot contain any special characters
- Cannot begin or end with a space
- Cannot contain your account number
- Cannot contain your first or last name
- Cannot be all numbers

Create a Username...

Set Username

### **ASSISTING A MEMBER WITH A USERNAME IN CU\*BASE**

There might be occasions when the member forgets his or her username and contacts the credit union. The credit union will need to develop a policy for handling these situations.

In CU\*BASE the MSR has the option of viewing the username or simply deleting it. The MSR can use *Verify Member* (F1) to verify the member's identity before sharing any information. If the MSR deletes the username, the member will simply have to create a new one the next time he or she logs in to online banking.

Session 0 CU\*BASE GOLD Edition - ABC CREDIT UNION



File Edit Tools Help

## Update Audio/Online Banking Access UPDATE

Account JOHN M MEMBER

---

The Member is Allowed to Access This Account Using

 <input checked="" type="checkbox"/> Online banking Reason D02 ⓘ	 <input checked="" type="checkbox"/> Audio response Reason D02 ⓘ
---	--

### Change Password


- ☐ Reset password to the last four digits of the member's SSN & the member's 4 digit birth year  
Reason D02 ⓘ
- ☐ Assign a custom password

[Reset Security Questions](#)

Date the member last logged into online banking  
**Nov 04, 2013**


Date the member accepted the online banking use agreement  
**Mar 02, 2010**

☒ Member has a PIB profile

 For organizations, the first 2 letters of the organization are used when resetting the password.

### Change PIN

- ☐ Reset PIN to last four digits of member's SSN  
Reason D02 ⓘ
- ☐ Assign a custom PIN

<a href="#">Verify Member</a>	 <a href="#">Skip</a>	<a href="#">Password History</a>	<a href="#">PIB</a>	<a href="#">Reset Security Quest</a>	<a href="#">Theme</a>
<a href="#">Start Page</a>	<a href="#">Photo Album</a>	<a href="#">Display Username</a>			

⏪ ⏩ ↶ ⏸ 📄 🔗 ⓘ ? @
FR (3723) 11/04/13 \*

Once *Display Username* (F20) is selected, the MSR can view the username and confirm the member's identity using *Verify Member* (F1). The MSR can then use *Delete Username* (F16) if needed.

# STATEMENT SECURITY

## ONLINE BANKING INDEMNIFICATION NOT REQUIRED FOR ESTATEMENTS

Once a member is enrolled in eStatements, the system begins generating eStatements for the member. The member does not need to log into online banking and accept the Online Banking Use Agreement. To audit the creation of eStatements to only members who have logged into online banking, use the batch unenroll feature covered in the next section of this booklet.

## BATCH MEMBER UN-ENROLLMENT

You can unenroll members from eStatements using the feature below. This feature lets you gather a batch of members according to their e-Statement enrollment status, compared to either their Use Agreement acceptance date, or their last logged in date, or even the status of their email address, and then elect to un-enroll them from e-Statements all at the same time. This screen allows you to run an Audit and prints a corresponding report. After evaluation, select the Update mode.

### ***e-Statement Batch Un-enrollment (Tool #365)***

Session 0 CU\*BASE GOLD Edition - Batch Un-enroll Members from E-Statements

Corp ID 01

Report Options	Response
Processing type	<input checked="" type="radio"/> Audit <input type="radio"/> Update
<input checked="" type="checkbox"/> Print report	
<input type="checkbox"/> Export to file	

Online banking use agreement last updated on Jan 27, 2010

Online banking passwords expire after 90 days of non-use.

Membership qualifications un-enroll members with an e-statement enrollment date PRIOR TO 00000000 [MMDDYYYY]

That have:

- ☐ Not accepted the use agreement
- ☐ Not logged into the online banking in over 000 days
- ☐ Bad email address

Navigation icons: < > ↑ ↓ ⌂ ⌕ ? @

FR (4339)

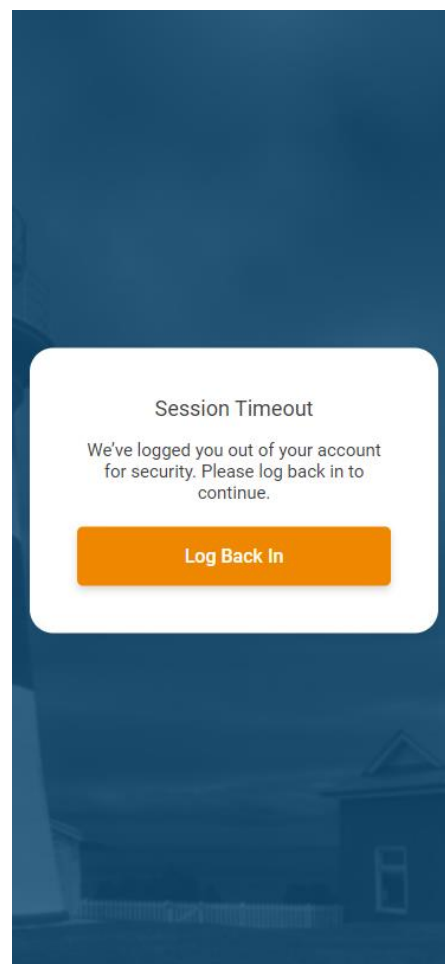
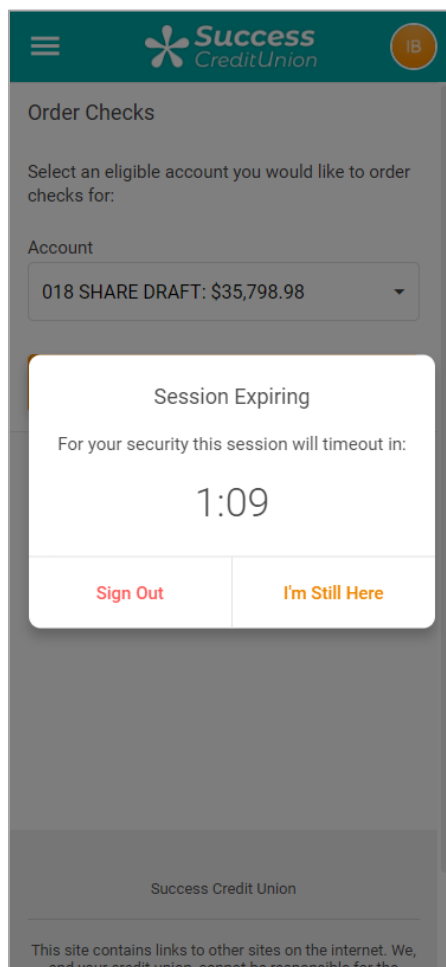
---

# TIMEOUT NOTIFICATION

As a security feature, members are automatically logged out of **It's Me 247** after fifteen minutes of inactivity or page refresh. (The login and security screens are the only exceptions. Members are logged out of them after five minutes of inactivity.)

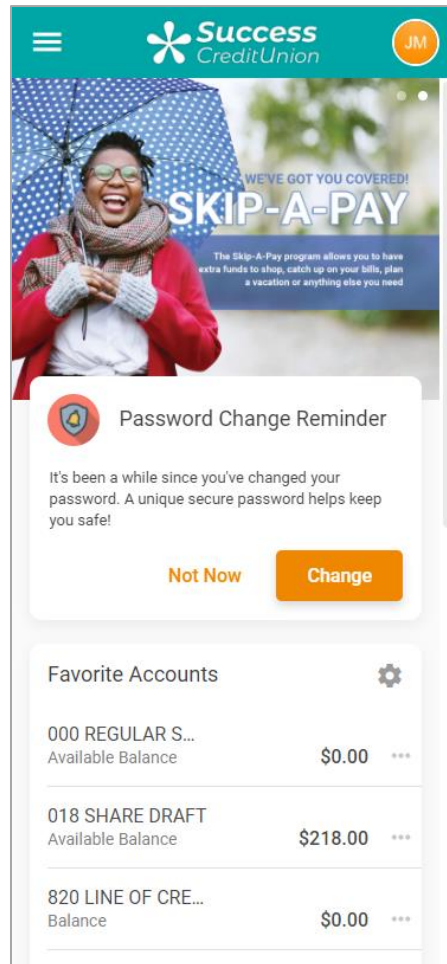
Members are alerted after twelve minutes of inactivity with a pop-up window that counts down the remaining three minutes. If the member clicks "I'm Still Here," the timer will be reset, and the page will not be refreshed (so the member will not lose anything they have done on the page). If the user does not respond or clicks "Sign Out," they are automatically logged out of **It's Me 247**.

## "It's Me 247" Timeout Notification



# PASSWORD CHANGE REMINDERS

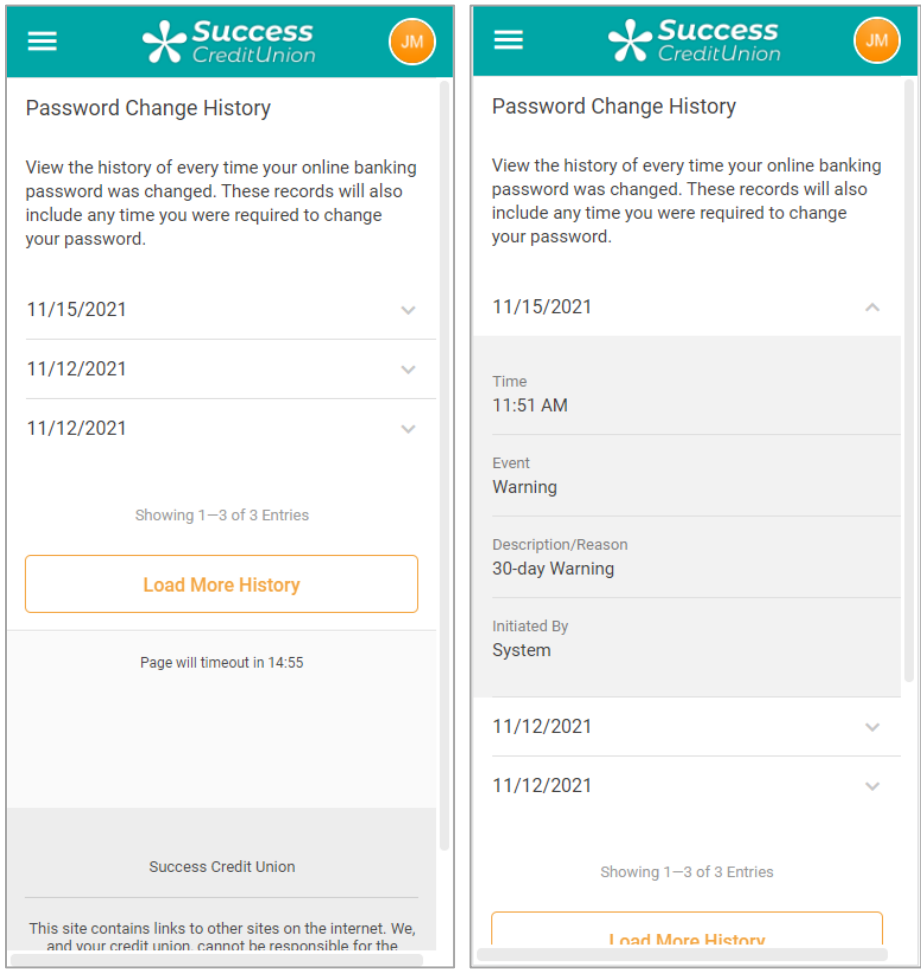
**It's Me 247** displays automated “soft” warning messages to members to encourage them to change their password on a regular basis, without making it mandatory. These soft warning messages appear when a member has not changed their password for the prior thirty days.



Members can select *Change* which navigates them directly to the screen where they can change their password. They can also select *Remind me later*. In this case the warning disappears for thirty days. If they do nothing, the warning will remain at the top of the page.

Members can view their selections on a “Password Change History page available from the “Personal Info & Settings” section in online banking. If they click the down arrow, the detail of the password change appears.

**Password Change History and Detail**



Members changes are recorded in CU\*BASE on the PIN/Password change dashboard. **See Page 53.**

---

# PERSONAL INFORMATION CHANGE NOTIFICATIONS

To comply with Red Flag requirements to monitor things like address changes, **It's Me 247** and CU\*BASE provide alerts to both the credit union and the member when changes are made to a member's personal information to provide an extra layer of security against fraudulent activity.

## Note on Credit Union Review of Change

Credit unions can select to have the member's changes in the Personal Information area in **It's Me 247** to be automatic or they can set it so that the credit union first needs to review the member's change through **Tool #13 Work Online Banking Apps/Req.** If the credit union selects to review the changes, the emails and online banking messages (mentioned in the next section) will not be sent until the credit union accepts the change.

[Credit unions can require that changes made by members in the Personal Information page in online banking be approved before they are updated in the system. What special conditions do not require an email address to be reviewed?](#)

## CHANGES TO ONLINE BANKING PASSWORD AND EMAIL

Both an online banking message and email confirmation are sent (to the email address on file for the member) whenever he or she change his or her online banking password, either via **It's Me 247** or with the help of a credit union employee via CU\*BASE. These messages and emails are sent automatically. This is a security feature that is intended to warn members if someone else initiates a password change on their accounts without their knowledge. An online banking confirmation message is also sent.

The system generates two confirmation emails any time an employee makes a change to his or her email address in **It's Me 247** (one to the old email address and one to the new email address).

An example of the email confirmation messages sent is shown below. This is the content of the email sent if a member changes his or her online banking password. The text changes slightly if the change was made in CU\*BASE.

Your online banking password was changed 08/04/10. For your protection we are sending this message as confirmation to verify that this change was made according to your instructions.

If you did not initiate this change, please contact your credit union immediately. Remember that if you have more than one membership at the credit union, the change may only have affected one of these accounts.

ABC Credit Union  
616-555-1212  
www.abccreditunion.com

This email contains the credit union's Signature Line (SL) message to further confirm the message has come from the credit union. This is configured in

the Master Message Center. (Refer to the *Marketing Campaigns with Member Connect* booklet on the CU\*BASE Reference Page for details.)

HINT: This is another reason why it is so important for staff to carefully verify a member's identity when resetting passwords, and to have extra controls in place if someone wants them to update both an email address AND reset a password at the same time. Could be a bad guy!

If an employee changes the information via CU\*BASE, the member will receive a similar message with slightly different wording. The online banking confirmation message the member receives has wording similar to the email message.

## PERSONAL INFORMATION CHANGES

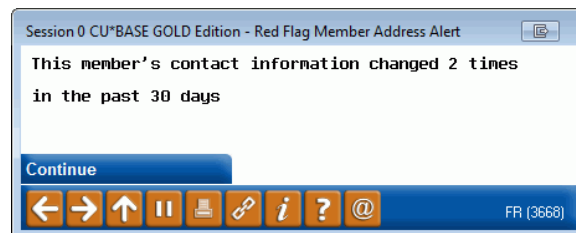
If the member makes any changes to the other information included on the *Personal Information* page in **It's Me 247**, the system generates an online banking confirmation message. These messages are sent both if the change is made by the member online or by an employee in CU\*BASE.

Personal Information changes that receive an online banking confirmation include:

- Address Line 1
- Address Line 2
- City
- State
- Zipcode
- County
- Home Phone
- Work Phone
- Other Phone
- Fax Phone
- Code Word

## RED FLAG WARNINGS IN CU\*BASE FOR EMPLOYEES

When credit union employees enter selected screens (such as Teller, Inquiry and Phone Operator), they receive a warning message noting how many changes have been made to these personal information items in the last 30 days.



Each time a change is made to the member personal information, a Tracker entry is made on the Audit Tracker that records the old and new values. The Tracker also notes if the Employee ID of the person who made the change in CU\*BASE, or 96 if the change was made in online banking.

- NOTE: CASS Certification does not trigger this red flag feature.



This feature is activated using **Tool #750 Red Flag Controls**.

Session 0 CU\*BASE GOLD Edition - Configure Audit/Red Flag Alerts

**Auto-Display Contact Info Change Alert**

Auto-display message in

☒ Teller    ☒ Inquiry    ☒ Phone

☐ Payroll    ☐ ATM/debit card maintenance

☐ Update/order online credit cards

☒ Member personal banker

☐ ATM/DR card activity inquiry

Days to display message

FR (3677)

This configuration allows the credit union to select which CU\*BASE options will display the message in CU\*BASE, including:

- Teller
- Inquiry
- Phone Operator
- Payroll – **Tool #504 Member Payroll Inquiry**
- ATM/Debit card maintenance – **Tool #11 ATM/Debit Card Maintenance**
- Updating/ordering credit cards – **Tool #12 Update/Order Online Credit Cards**
- Member Personal Banker (**Tool #14 Member Personal Banker**)
- ATM/DR card account activity (**Tool #156 ATM/Debit Cards & Activity Inquiry**)

Additionally, the configuration allows the credit union to configure the number of days that the warning message will appear in CU\*BASE.

- NOTE: When instituting this feature, be sure to provide your staff with training on what to do if they see the Red Flag message. Should they ask for photo identification to confirm the address?

---

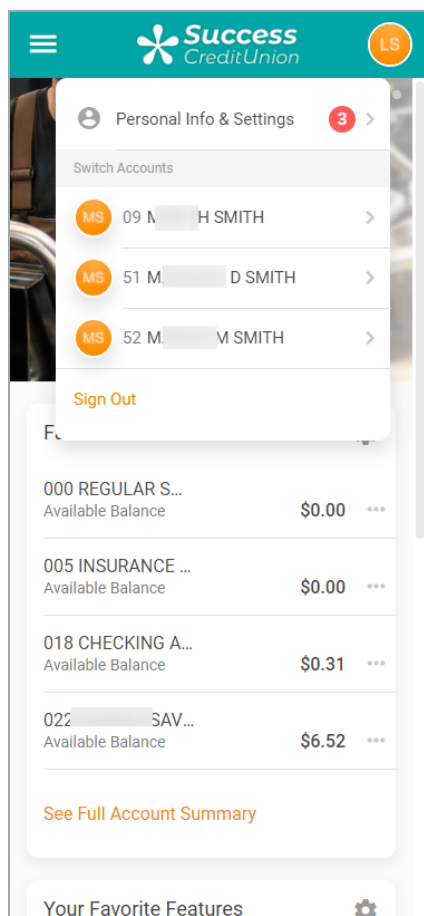
# JUMP ACCESS CONTROLS

To learn more about this feature, be sure to check out the Jump Controls booklet, located on the **It's Me 247** reference page:

<https://www.cuanswers.com/wp-content/uploads/SeeJumpControls.pdf>

In a nutshell, once this feature is activated and the appropriate permissions are given, the member can “jump” to another account. Your biggest user of Jump will probably be a member with multiple memberships at your credit union.

Jump allows a member to log into one of their memberships and then jump to another of their memberships (same SSN) without additional authentication. Members can also grant Jump permissions to any other joint owner on their base (000) account, such as a spouse, who also has a credit union membership. From here, with a few exceptions such as applying for a loan, viewing checks, or changing a password, it is as if they logged into this second account; they can make transfers, schedule AFTs, change preferences, and more.



For a more in depth look at this discussion, which forms the basis for the decision to only give access to owners via Jump, refer to this Answer Book discussion:

<https://kb.cuanswers.com/cuanswers/consumer/kbdetail.asp?kbid=3665>

---

# INTER-MEMBER TRANSFER CONTROLS

## OVERVIEW

Inter-Member Transfers allow members to transfer to other members at your credit union. These transfers are done via the Transfer Wizard in online banking. Two options exist for inter-member transfers: transfer control lists and direct account input.

You credit union can select to activate either one or both of the inter-member transfer options. To activate this feature, fill out an **It's Me 247** Configuration Change Request and fax it to the Client Services Department. This document is located on the **It's Me 247** Reference Page. *Self Processors: This setting is located via **OPER Tool #5356 Online Banking Configuration**.*

## TRANSFER CONTROL LISTS

Transfer Control lists are used to control which of your credit union memberships a member can transfer to via the Transfer Wizard. These accounts are the only accounts a member can use when setting up an ACH Distribution or Automated Funds Transfer (AFTs) in online banking, or when making a transfer in Mobile Banking. The benefit of the Transfer Control lists for members is that these memberships appear in a handy list for them to choose from so they don't need to remember their friends' and family's account numbers.

The benefit of Transfer Control lists for credit unions is that they control the addition of memberships to the member's Transfer Control list. Credit unions add memberships to a member's Transfer Control list via **Tool #883 Update ARU/Online Banking Transfer Ctrl.** A member cannot add an account to his or her Transfer Control List while in online banking.

## DIRECT ACCOUNT INPUT

Direct Account Input allows the member to enter the account and suffix directly on the Transfer Wizard page when making the transfer. They are also required to enter the first three letters of the last name of the member they are transferring to prevent incorrect entry. This might be used by the member for transfers to accounts they do not transfer to frequently or that they do not want to add to their Transfer Control list.

## INTER-MEMBER TRANSFERS: WHAT THE MEMBER SEES IN ONLINE BANKING

Below is an example of what a member might see if a credit union activated both Inter-Member Transfer options. Credit unions can select to offer either one or both of the options.

- In the example below, Lisa Smith is on this member's Transfer Control list.

Success Credit Union MS

Quick Transfer

Transfer From

000 REGULAR SHARE: \$1,887.10

Transfer To

Select an Account...

Select an Account...

My Accounts

018 CASH: \$990.28

xx1793 PLATINUM: \$0.00

xx8641 PLATINUM: \$275.43

L SMITH

000 REGULAR SHARE (...85)

005 INSURANCE ACC (...85)

018 CHECKING ACC (...85)

022 SAVER (W/CB) (...85)

Accounts at Other Financial Institutions

Another Member

Success Credit Union

This site contains links to other sites on the internet. We, and your credit union, cannot be responsible for the

# EVALUATING THE REASON FOR A PASSWORD CHANGE

Maybe you want to pinpoint why a member's password has changed in **It's Me 247**. Did the member change the password or ask a MSR to change it to a specific password? Was the account disabled because the member entered an incorrect password too many times? Did an MSR change the password temporarily to the last four digits of the member's social security number? Did the member follow that action by changing the password to one he or she chose? Answer these questions using the Member PIN Password Change online report via **Tool #505 Member PIN/Password Change History**. Select a Password Type of WWW (online banking) and the online report shows how many times and why a member's online banking password was changed.

This dashboard also records the warnings the member receives to remind them to periodically change their password as well as if they choose to ignore the warning. See **Page 45** for details and what the member sees in online banking.

Use *Print* (F14) to print a report of the items.

## Member PIN/Password Change History (Tool #505)

Session 0 CU\*BASE GOLD - ABC CREDIT UNION

File Edit Tools Help

### PIN/Password Member History Inquiry

Filter by

Date range From  to  [MMDDYYYY]

Change code  Change reason

Password type  Account base

Program name  Employee ID

Account Base	Date	Time	Change Code	Reason	Password Type	Program Name	Emp ID
	Mar 16, 2015	14:36:43	Changed	Reset by CU	WWW	UPIN	-1
	Mar 16, 2015	14:37:31	Changed	Reset by CU	IVR	UPIN	-1
	Mar 17, 2015	15:58:04	Warning	30-day Warning	WWW	PAHTC502	96
	Mar 18, 2015	09:14:46	Warning	30-day Warning	WWW	PAHTC502	96
	Mar 31, 2015	11:08:39	Reset	Reset by CU	WWW	UPIN	;D
	Mar 31, 2015	11:09:22	Reset	Reset by CU	WWW	UPIN	;D
	Mar 31, 2015	11:10:05	Forced change	Changed by Mbr	WWW	PAHTC502	96
	Mar 31, 2015	13:01:02	Reset	Reset by CU	WWW	UPIN	;D
	Mar 31, 2015	13:02:28	Reset	Reset by CU	WWW	UPIN	;D
	Mar 31, 2015	13:03:22	Forced change	Changed by Mbr	WWW	PAHTC502	96
	Apr 08, 2015	15:13:20	Reset	Reset by CU	WWW	UPIN	-1
	Apr 08, 2015	15:13:31	Changed	Reset by CU	WWW	UPIN	-1
	Apr 09, 2015	11:56:10	Changed	Reset by CU	WWW	UPIN	-1
	Apr 13, 2015	09:40:17	Disabled	Reset by CU	IVR	UPIN	+4
	Apr 13, 2015	09:40:17	Disabled	Disabled by CU	WWW	UPIN	+4

Clear Filter

Print

Aggregate

FR (5661) 4/15/15

# EVALUATING YOUR MEMBERSHIPS

## WITHOUT ACTIVITY

You may choose to keep tabs on your members who have logged into online banking at one time, but have not logged in again during the period of time you have configured for non-use expiration.

- NOTE: The longest period a member might appear on this list would be 90 days, which is the maximum period you can set for password expiration due to non-use. The length of the expiration days is set in the *Online/Mobile Password and Security Settings*. (See page 19.)

To keep an eye on members who are activated but have not logged into **It's Me 247** in a while use **Tool #161 Audit Disabled/Inactive PIN/PWs Rpt.** The report allows you to specify a range of "last login dates" and view the members who are active, but have not used online banking during that time. For example, you might pull a list of all accounts with a last logged in date greater than two month ago. You may decide to set up a personal contact or direct mail campaign to encourage them to try online banking again.

### Audit Disabled/Inactive PIN/PWs Rpt (Tool #161)

### Report Sample

1/18/10 09:43:00		TEST CREDIT UNION					LPWDCALLST		PAGE	1
DISABLED ONLINE BANKING MEMBER CONTACT LIST										
ALYCIAM										
LAST LOG ON BEGINNING DATE: 11/01/2009 TO LAST LOG ON ENDING DATE: 1/18/2010										
ORDERED BY DAYS SINCE LAST LOGIN										
ACCOUNT				LAST LOG-IN	LAST CHANGED	DAYS SINCE	STALE	DISABLED	CHALLENGE	
BASE	MEMBER NAME	PHONE NUMBERS		DATE	DATE	LAST LOG-IN	PASSWORD	PASSWORD	QUSTN/ANS	
7916	SHANNON L MEMBER	Home: 555-555-5555		11/02/2009	11/05/2009	77		Y	Y	
		Work: 222-2222			smember@cuanswers.com					
38810	CARISSA J MEMBER	Home: 777-777-7777		11/04/2009	11/20/2009	75		Y	Y	
		Work: 777-888-8888			cmember@cuanswers.com				Y	

## REVIEW YOUR CREDIT UNION PLAN AND PROCEDURES

Regardless of which CU\*BASE and **It's Me 247** tools you choose to use, the point is to make sure your credit union has a *plan* and procedures in place to monitor and control your members' access to online banking. Contact Client Services if you would like assistance in setting up some custom reports or inquiries, or in changing any of your existing configuration settings.

---

## **APPENDIX A: ONLINE BANKING USE AGREEMENT**

Following is the verbiage of the Online Banking Use Agreement.

# Online Banking Use Agreement, Authorization to Receive Electronic Statements and Other Disclosures, and Electronic Bill Payment

1. The **It's Me 247** online banking system (hereinafter called the SYSTEM), is provided as a service of the CREDIT UNION and permits access to your account information and, upon request, allows account transactions to be conducted. By accessing the SYSTEM, you are verifying that you are the account holder or you have full legal authority granted by the account holder to obtain information and conduct transactions. Reference to "computer" in this Agreement shall mean any electronic and/or digital device that provides web browser capabilities, including personal computer, laptop, personal digital assistant, and mobile and/or smartphone compatible with the SYSTEM.
2. The CREDIT UNION has provided an Account Number and initial password which are required to permit access through the SYSTEM. The first time you login the SYSTEM, you will be required to change this initial password. You authorize the CREDIT UNION to follow any instructions entered through the online banking SYSTEM using your password. You agree that you are responsible to make sure that the Account Number and password are maintained in a secure manner and not disclosed to any person who is not authorized to obtain account information or conduct transactions on your account.
3. If you use any method of storing the Account Number and password on your computer, you agree that you are solely responsible for any access obtained to account information or any transactions conducted on any account. If you have reason to believe that the Account Number or password have been disclosed to or obtained by any unauthorized person, you agree to immediately notify the CREDIT UNION.
4. When connected to or using the SYSTEM, you agree to ensure that no unauthorized persons have access to your computer. If you fail to



maintain direct control and supervision over your computer or otherwise fail to ensure that no unauthorized persons have access to your computer when connected to or using the SYSTEM, you agree that any use of the SYSTEM utilizing your password is not unauthorized use, and the CREDIT UNION and any other companies or entities involved in the design, development or operation of the SYSTEM are not responsible for any loss, expense, injury, cost or damage resulting from any access obtained to account information or any transactions conducted on any account, to the extent permitted by law.

5. CREDIT UNION may provide documents which are delivered to you electronically. These electronic documents are accessible when you login to the online banking SYSTEM. You agree to receive these documents, and any disclosures to which you are entitled under Federal Reserve Board Regulations B (Equal Credit Opportunity Act), E (Electronic Fund Transfers Act), M (Consumer Leasing Act), Z (Truth in Lending Act), and CC (Expedited Funds Availability Act); the National Credit Union Administration Truth in Savings Regulation, the Fair Credit Reporting Act, and any other applicable state or federal regulation or statute, including but not necessarily limited to your monthly CREDIT UNION account statement, electronically, through your access to this system.
6. You understand and acknowledge that you presently have the right to receive such disclosures in paper form, and that you may revoke the authorization given in Section 5 at any time by providing CREDIT UNION with written notice of such revocation, at which time you will again be entitled to receive such disclosures in paper form. Whether you send such notice of revocation by paper or electronic means, the effective date of your revocation will be no more than 30 days from the day such notice is acknowledged as received by CREDIT UNION.
7. To access and retain your eStatements and other electronic disclosures, you must meet the following technical requirements. You must have Internet access and a valid email account and address. You must request access to the online banking SYSTEM through the CREDIT UNION. Your computer must have installed browser software currently supported by the SYSTEM and utilizes appropriate security protections. If you fail to use current, supported browser software, the CREDIT UNION and any other entities involved in the design, development or operation of the SYSTEM are not responsible for any loss, expense, injury, cost or damage resulting from any access obtained to account information or any transaction conducted on any account. For eStatements and other electronic documents, you must

have access to a printer or the ability to download information to keep copies of electronic documents for your records.

8. You understand and agree that you must notify CREDIT UNION if your email address changes, by providing the CREDIT UNION with written or electronic notice of any such change in address, and that the effective date of this new email address will be no more than 30 days from the day such notice is acknowledged as received by CREDIT UNION. You hereby hold the CREDIT UNION harmless in the event that you have not received any required statement or other notice as a result of your failure to notify the CREDIT UNION of a change in your email address.
9. You understand and agree that even though you have agreed to receive disclosures electronically, you may contact the CREDIT UNION by email or telephone to request that the CREDIT UNION send a paper copy of a disclosure that has already been sent electronically, and that the CREDIT UNION may charge a fee for that service, which fee will be separately disclosed. You agree that such fee can be deducted by the CREDIT UNION from any account you own at the CREDIT UNION.
10. CREDIT UNION may amend the terms of this Agreement by giving you notice of the amendment. Your continued use of the SYSTEM after such notice is given constitutes your agreement to the amendments.
11. By accepting this Agreement, you acknowledge that you have read the terms of this Agreement and that you agree to be bound by these terms. When you enroll in the eStatement service, you consent to receive your periodic account statements and other disclosures electronically. If your CREDIT UNION account is owned jointly with another person(s), any one of you may consent to receive eStatements and electronic disclosures, including eNotices. Further, you understand that by accepting this Agreement, the current date will be logged as part of your account records and the SYSTEM services will be activated for your account.

**\*\*\* The Following Sections Only Apply to Users of the  
PAYVERIS BILL PAY SYSTEM \*\*\***

## **Payveris Bill Pay Terms and Conditions**

### **1. Service Definitions.**

"Agreement" means these Terms and Conditions of the CREDIT UNION Bill Pay Service.

"Biller" is the person or entity to which you wish a bill payment to be directed or is the person or entity from which you receive electronic bills (E-Bills), as the case may be.

"Billing Account" is the checking account from which all Service fees will be automatically debited.

"Business Day" is every Monday through Friday, Eastern Time, excluding Federal Reserve holidays.

"Disclosures" means terms, conditions, and other information required to be communicated to you by law.

"Due Date" is the date reflected on your Biller statement for which the payment is due. It is not the late date or grace period.

"External Transfers" means when you transfer funds out of your CREDIT UNION account for credit to an external account at another financial institution.

"Payment Instruction" is the information provided by you to the Service for a bill payment to be made to the Biller (such as, but not limited to, Biller name, Biller account number, and Scheduled Payment Date).

"Payment Account" is the checking account from which bill payments will be debited.

"Scheduled Payment" is a payment that has been scheduled through the Service but has not begun processing.

"Send Date" means the day the payment is sent and your account is debited. For payments sent by check, your account will be debited when the check is presented for payment.

"Service" means the Bill Pay Service offered by the CREDIT UNION, through our designated service provider.

"Service Provider" means companies that we have engaged to render some or all of the Service to you on our behalf.

2. To access and retain copies of your online statements and to utilize the Payveris Bill Pay System and to receive other related notices, you must have Internet access with a compatible browser. You may also need a PDF reader. You are solely responsible to obtain compatible hardware and software.
3. If our hardware or software requirements change, and that change would create a material risk that you would not be able to access or retain your electronic records, we will give you notice of our revised hardware and software requirements. Continuing to use our online and electronic bill paying services after receiving notice of the change is reaffirmation of your consent to use electronic records and to transact electronically.
4. There is no limit on the number of transfers from your savings account or your Money Market Savings Account if they are made in person, by Automatic Teller, or by mail, or if they are made to make monthly payments on the CREDIT UNION loans, to have funds mailed directly to you, or as a distribution of your Direct Deposit.

Federal regulations limit the number of certain types of transfers and/or withdrawals you can make from your savings account and your Money Market Savings Account to six per calendar month. The types of transfers that are limited are those requested by fax, telephone, internet, and pre-authorized transfers.

5. The terms and conditions of these services are subject to change without notification to you, unless prior notification is required by law. CREDIT UNION reserves the right to revoke or refuse Account Access or Mobile Banking services.

We may cancel your Account Access services at any time with or without written notice to you. For example (and not excluding other examples), if you do not provide us with your current mailing address and email address, we may cancel your services until you provide us with your current addresses.

### **Your Liability for Unauthorized Transfers**

6. **Liability Disclosure.** By applying for Account Access, you agree to accept responsibility for protecting the integrity of your Password, Password Reset Question and Answer, and Challenge Questions and Answers. To help prevent unauthorized transactions and/or account access, you also agree to ensure the security of the personal computer (PC) you own and/or use to

access the CREDIT UNION Account Access service. By securing the PC you own and/or use, we specifically mean installing antivirus software, a firewall, and spyware detection software on your PC, and keeping this security software current, or verifying that the above security software has been installed and is current. You also agree that the CREDIT UNION may revoke Account Access if unauthorized account access occurs as a result of your negligence in safeguarding the Password, Password Reset Question and Answer, and Challenge Questions and Answers, or as a result of your negligence in ensuring the security of the personal computer you own and/or use to access the Account Access service, as described above. Further, you agree that, if the CREDIT UNION is notified that you have included CREDIT UNION in the filing of a petition of bankruptcy, CREDIT UNION may revoke or refuse Account Access service. Granting access to your account via the Internet to a non-signer on the applicable account(s) will make you financially liable for all unauthorized access, losses, or misuse of the account until reported to the CREDIT UNION.

Notify us AT ONCE if you believe your account has been accessed without your authority. The best way to minimize your possible loss is to telephone, although you may advise us in person or in writing. If you do not notify us, you could lose all the money in your account (plus your maximum line of credit amount). If you tell us within two (2) business days of learning of unauthorized access, you can lose no more than \$50 if someone accesses your account without your permission. If you do NOT tell us within two (2) business days of learning of the unauthorized access, and we can prove that we could have prevented it if you had provided us proper notification, you could lose as much as \$500.

If your statement shows any electronic fund transfer you did not make or authorize, advise us at once. If you do not tell us within sixty (60) days after the statement was delivered to you of any unauthorized or fraudulent use of your account, you may be liable for money lost after the sixty (60) days.

If a good reason (such as a long trip or a hospital stay) prevents you from notifying us, we may extend time periods.

### **Documentation of Transactions**

- 7. Periodic Statements.** You will receive a monthly account statement for each month in which you initiate electronic transactions via Payveris Bill Pay Service, unless you choose to suppress your statement. At a minimum, you will receive a quarterly savings account statement. Additionally, you can view your savings and checking transaction activity through Account Access.

**8. Transaction Fees.** The CREDIT UNION does not charge for transfers initiated via Account Access, viewing account information via the Internet, or the companion Bill Pay services. CREDIT UNION reserves the right to charge for Account Access or Bill Pay. You will be given at least 21 days advance notice before the CREDIT UNION implements any new fees for Account Access or Bill Pay.

**9. Liability for Failure to Make Transfers.** If the CREDIT UNION does not complete a transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will NOT be liable, for instance, if, through no fault of ours, you do not have sufficient funds in your account or available credit in your line of credit to make the transfer; if the funds in your account are subject to legal process, such as garnishment or attachment; if the account is subject to a pledge or security agreement; or if, despite reasonable precautions that we have taken, circumstances beyond our control (such as fire, power failure, flood, or failure of paying agency to deliver direct deposit payment data) prevent the transfer.

**10. Account Information Disclosure.** We will disclose information to third parties about your account or the transactions you make:

- If we return checks on your account drawn on non-sufficient funds or if we are unable to complete an electronic transfer because of non-sufficient funds.
- When it is necessary for completing transfers.
- To verify the existence or conditions of your account for a third party, such as a credit bureau or merchant.
- To comply with government agency or court orders.
- If you give us your written permission.
- In accordance with our privacy policy.

### **In Case of Errors or Questions About Your Electronic Transfers**

**11.** If you think your statement or receipt is wrong, or if you need more information about a transaction listed on the statement or receipt, contact CREDIT UNION as soon as possible.

- We must hear from you no later than sixty (60) days after the FIRST statement on which the problem or error appeared.
- Tell us your name and account number.
- Describe the error or the transaction you are unsure about and explain as clearly as you can why you believe it is an error or why you need more information.
- Tell us the dollar amount of the suspected error.
- If you tell us orally, we may require that you send your complaint or question in writing within ten (10) business days. We will notify you of the results of our investigation within ten (10) business days (twenty [20] business days for new accounts) of hearing from you, and we will correct any error promptly. If we need more time, however, we may take up to forty-five (45) days to investigate your complaint or question. If we decide to do this, we will provisionally credit your account within ten (10) business days (twenty [20] business days for new accounts) for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. A provisional credit is a temporary credit adjustment made to your account during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within ten (10) business days, we may remove the provisional credit from your account. Please note that contacting us by telephone will not preserve your rights. If it is determined that there was no error, we will send you a written explanation within three (3) business days of completing our investigation, and any provisional credits will be reversed. If you do not have sufficient funds in your account to cover the amount of the provisional credit, the account will be overdrawn, and you will be responsible for payment. You may ask for copies of the documents that we used in our investigation.

**12.** To help fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account, including joint owners. When you open an account or become an authorized user, we will ask you for your name, address, date of birth, and other information that will allow us to identify you.

## **Use of the Bill Pay Service Provider**

- 13.** CREDIT UNION offers the Bill Pay service through our designated third-party service provider. The service provider will be processing bill payments and answering questions directly related to such member-initiated bill payments. Accordingly, the term "Customer Care" represents the customer service provided by the service provider to the CREDIT UNION Bill Pay subscribers on the CREDIT UNION behalf. CREDIT UNION, at its sole discretion, reserves the right to change Bill Pay service providers.
- 14.** Charges for the Bill Pay service, other transactions and optional services (e.g., non-sufficient funds or stop payment fees) can be found on the CREDIT UNION website or provided upon request.
- 15.** You agree to pay such fees and charges, and authorize the Service to charge your designated Billing Account for these amounts and any additional charges that may be incurred by you. Any fees associated with your share or loan accounts will continue to apply. You are responsible for any and all telephone access fees or Internet service fees that may be assessed by your telephone utility and/or Internet Service Provider.

### **Failed or Returned Transactions**

- 16.** In using the Service, you are requesting the Service to make payments for you from your Payment Account. If we are unable to complete the transaction for any reason associated with your Payment Account (for example, there are non-sufficient funds in your Payment Account to cover the transaction), the transaction will not be completed. In some instances, you will receive a return notice from the Service. In such case, you agree that:
- You will reimburse the Service immediately upon demand the transaction amount that has been returned to the Service;
  - For any amount not reimbursed to the Service within fifteen (15) days of the initial notification, a late charge equal to 1.5% monthly interest or the legal maximum, whichever rate is lower, for any unpaid amounts may be imposed;
  - You will reimburse the Service for any fees imposed by your financial institution as a result of the return;
  - You will reimburse the Service for any fees it incurs in attempting to collect the amount of the return from you; and



- The Service is authorized to report the facts concerning the return to any consumer credit reporting agency.

In these cases, you agree that a non-sufficient funds (NSF) fee will be charged in accordance with the CREDIT UNION'S published fees. Further, you also agree that a NSF fee may be charged to your account even if the payment is not returned but is paid and overdraws your Payment Account.

- 17.** By enrolling for and using the Service, you agree that the CREDIT UNION has the right to collect funds from all of your share accounts, as well as the available balance on your line of credit accounts (e.g., CLOC or credit card accounts) to recover funds for all payments that have been requested to be paid by you and your authorized user. This includes accounts on which you are the primary member-owner, as well as accounts on which you are the joint owner.

### **Bill Payment Scheduling**

- 18.** The earliest possible payment for each Biller (typically five [5] or fewer Business Days from the current date) will be designated within the application when you are scheduling the payment. Therefore, the application will not permit you to select a date less than the earliest possible date designated for each Biller. When scheduling payments, select a date that allows adequate time for delivery prior to any late date or grace period.
- 19.** For External Transfers the account debit will take place on the day the External Transfer is sent. When you transfer funds out of an external account at an external financial institution for credit to an account at CREDIT UNION, the account debit at the external financial institution will occur in accordance with ACH operating rules.

### **Prohibited Payments**

- 20.** The following types of payments are prohibited through the Service, and we have the right but not the obligation to monitor for, block cancel and/or reverse such payments:

Payments to persons or entities located in prohibited territories (including any territory outside of the United States); Payments that violate any law, statute, ordinance or regulation; Payments related to: (1) tobacco products, (2) prescription drugs and devices; (3) narcotics, steroids, controlled substances or other products that present a risk to consumer safety; (4) drug paraphernalia; (5) ammunition, firearms, or firearm parts or related accessories; (6) weapons or knives regulated under applicable

law; (7) goods or services that encourage, promote, facilitate or instruct others to engage in illegal activity; (8) goods or services that are sexually oriented; (9) goods or services that promote hate, violence, racial intolerance, or the financial exploitation of a crime; (10) goods or services that defame, abuse, harass or threaten others; (11) goods or services that include any language or images that are bigoted, hateful, racially offensive, vulgar, obscene, indecent or discourteous; (12) goods or services that advertise or sell to, or solicit others; or (13) goods or services that infringe or violate any copyright, trademark, right of publicity or privacy or any other proprietary right under the laws of any jurisdiction; Payments related to gambling, gaming and/or any activity with an entry fee and a prize, including, but not limited to casino games, sports betting, horse or greyhound racing, lottery tickets, other ventures that facilitate gambling, games of skill (whether or not it is legally defined as a lottery) and sweepstakes; Payments relating to transactions that (1) support pyramid or Ponzi schemes, matrix programs, other "get rich quick" schemes or multi-level marketing programs, (2) are associated with purchases of real property, annuities or lottery contracts, lay-away systems, off-shore banking or transactions to finance or refinance debts funded by a credit card, (3) are for the sale of items before the seller has control or possession of the item, (4) constitute money-laundering or terrorist financing; (5) are associated with the following "money service business" activities: the sale of traveler's checks or money orders, currency dealers or exchanges or check cashing, or (6) provide credit repair or debt settlement services; Tax payments and court ordered payments including but not limited to Alimony and Child Support.

In no event shall we or our independent contractors or other third parties to whom we assign or delegate rights or responsibilities be liable for any claims or damages resulting from your scheduling of prohibited payments. We have no obligation to research or resolve any claim resulting from a prohibited payment. All research and resolution for any misapplied, mis-posted or misdirected prohibited payments will be your sole responsibility and not ours. We encourage you to provide notice to us by the methods described in above of any violations of this section or the Agreement generally.

### **Payment Authorization and Payment Remittance**

- 21.** By providing the Service with names and account information of Billers to whom you wish to direct payments, you authorize the Service to follow the Payment Instructions that it receives through the payment system. In order to process payments more efficiently and effectively, the Service may edit or alter payment data or data formats in accordance with Biller directives.

**22.** When the Service receives a Payment Instruction, you authorize the Service to debit your Payment Account and remit funds on your behalf so that the funds arrive as close as reasonably possible to the Scheduled Payment Date designated by you. You also authorize the Service to credit your Payment Account for payments returned to the Service by the United States Postal Service or Biller, or payments remitted to you on behalf of another authorized user of the Service.

**23.** The Service will use its best efforts to make all your payments properly. However, the Service shall incur no liability, and any Service Guarantee shall be void if the Service is unable to complete any payments initiated by you because of the existence of any one or more of the following circumstances:

- If, through no fault of the Service, your Payment Account does not contain sufficient funds to complete the transaction or the transaction would exceed the credit limit of your CLOC account. Per federal regulation, pre-authorized telephone, Internet, or automatic transfers from savings to cover checking overdrafts cannot exceed six (6) in number per calendar month;
- The payment processing center is not working properly, and you know or have been advised by the Service about the malfunction before you execute the transaction;
- You have not provided the Service with the correct Payment Account Information, or the correct name, address, phone number, or account information for the Biller; and/or
- Circumstances beyond control of the Service (such as, but not limited to, fire, flood, or interference from an outside force) prevent the proper execution of the transaction, and the Service has taken reasonable precautions to avoid those circumstances.

Provided none of the foregoing exceptions are applicable, if the Service causes an incorrect amount of funds to be removed from your Payment Account or causes funds from your Payment Account to be directed to a Biller that does not comply with your Payment Instructions, the Service shall be responsible for returning the improperly transferred funds to your Payment Account, directing to the proper Biller any previously misdirected transactions, and, if applicable, any late payment-related charges.

**24.** The Service reserves the right to select the method in which to remit funds on your behalf to your Biller. These payment methods may include, but may not be limited to, an electronic payment or a laser draft payment (funds

remitted to the Biller are deducted from your Payment Account when the laser draft is presented to your financial institution for payment).

### **Payment Cancellation Requests**

- 25.** You may cancel or edit any Scheduled Payment (including recurring payments) by following the directions within the application. There is no charge for canceling or editing a Scheduled Payment. Once the Service has begun processing a payment, it cannot be canceled or edited. Therefore, a stop payment request must be submitted.
- 26.** The Service's ability to process a stop payment request will depend on the payment method and whether or not a check has cleared. The Service may also not have a reasonable opportunity to act on any stop payment request after a payment has been processed. If you desire to stop any payment that has already been processed, you must contact Bill Pay Customer Care, offered through our Service Provider. Although the Service will make every effort to accommodate your request, the Service will have no liability for failing to do so. The Service may also require you to present your request in writing within fourteen (14) days. Please refer to the CREDIT UNION'S fees, which can be found on the CREDIT UNION website.

### **Electronic Bill (E-Bill) Delivery and Presentment**

- 27.** This feature is for the presentment of electronic bills (E-Bills) only, and it is your sole responsibility to contact your Billers directly if you do not receive your statements. In addition, if you elect to activate one of the Service's electronic bill options, you also agree to the following:
- **Information provided to the Biller** – The Service is unable to update or change your personal information such as, but not limited to, name, address, phone numbers, and email addresses with the electronic Biller. Any changes will need to be made by contacting the Biller directly. Additionally, it is your responsibility to maintain all usernames and passwords for all electronic Biller sites. You also agree not to use someone else's information to gain unauthorized access to another person's bill. The Service may, at the request of the Biller, provide to Biller your email address, service address, or other data specifically requested by the Biller at the time of activating the electronic bill for that Biller, for the purposes of the Biller informing you about Service and/or bill information.

- **Activation** – Upon activation of the electronic bill feature, the Service may notify the Biller of your request to receive electronic billing information. The presentment of your first electronic bill may vary from Biller to Biller and may take up to sixty (60) days, depending on the billing cycle of each Biller. Additionally, the ability to receive a paper copy of your statement(s) is at the sole discretion of the Biller. While your electronic bill feature is being activated, it is your responsibility to keep your accounts current. Each electronic Biller reserves the right to accept or deny your request to receive electronic bills.
- **Authorization to obtain bill data** – Your activation of the electronic bill feature for a Biller shall be deemed by us to be your authorization for us to obtain bill data from the Biller on your behalf. For some Billers, you will be asked to provide us with your username and password for that Biller. By providing us with such information, you authorize us to use the information to obtain your bill data.
- **Notification** – The Service will use its best efforts to present all of your electronic bills promptly. In addition to notification with the Service, the Service may send an email notification to the email address listed for your account. It is your sole responsibility to ensure that this information is accurate. In the event you do not receive notification, it is your responsibility to periodically log in to the Service and check on the delivery of new electronic bills. The time for notification may vary from Biller to Biller. You are responsible for ensuring timely payment of all bills.
- **Cancellation of electronic bill notification** – The electronic Biller reserves the right to cancel the presentment of electronic bills at any time. You may cancel electronic bill presentment at any time. The timeframe for cancellation of your electronic bill presentment may vary from Biller to Biller. It may take up to sixty (60) days, depending on the billing cycle of each Biller. The Service will notify your electronic Biller(s) as to the change in status of your account, and it is your sole responsibility to make arrangements for an alternative form of bill delivery. The Service will not be responsible for presenting any electronic bills that are already in process at the time of cancellation.
- **Non-delivery of electronic bill(s)** – You agree to hold the Service harmless should the Biller fail to deliver your statement(s). You are responsible for ensuring timely payment of all bills. Copies of previously delivered bills must be requested from the Biller directly.

- **Accuracy and dispute of electronic bill** – The Service is not responsible for the accuracy of your electronic bill(s). The Service is only responsible for presenting the information we receive from the Biller. Any discrepancies or disputes regarding the accuracy of your electronic bill summary or detail must be addressed with the Biller directly.

This Agreement does not alter your liability or obligations that currently exist between you and your Billers.

## **Security**

- 28.** You agree not to give or make available your password or other means to access your account to any unauthorized individuals. You are responsible for all payments you authorized using the Services. If you permit other persons to use the Service or your password or other means to access your account, you are responsible for any transactions they authorize. If you believe that your password or other means to access your account has been lost or stolen, or that someone may attempt to use the Service without your consent or has transferred money without your permission, you must notify the Service at once.
- 29.** If you tell us within two (2) Business Days after you discover your password or other means to access your account has been lost or stolen, your liability is no more than \$50.00 should someone access your account without your permission. If you do not tell us within two (2) Business Days after you learn of such loss or theft, and we can prove that we could have prevented the unauthorized use of your password or other means to access your account if you had told us, you could be liable for as much as \$500.00. If your monthly financial institution statement contains transfers that you did not authorize, tell us at once. If you do not tell us within sixty (60) days after the statement was delivered to you of any unauthorized or fraudulent use of your account, you may be liable for money lost after the sixty (60) days. If a good reason (such as a long trip or a hospital stay) prevented you from telling us, we may extend the period.

## **Errors and Questions**

- 30.** In case of errors or questions about your transactions, you should notify CREDIT UNION as soon as possible.
- 31.** If you think your statement is incorrect or you need more information about a Service transaction listed on the statement, CREDIT UNION must hear

from you no later than sixty (60) days after the FIRST statement was sent to you on which the problem or error appears. You must:

- Tell the CREDIT UNION your name and Service account number;
- Describe the error or the transaction in question and explain as clearly as possible why you believe it is an error or why you need more information; and
- Tell CREDIT UNION the dollar amount of the suspected error.

If you tell CREDIT UNION verbally, the CREDIT UNION may require that you send your complaint in writing within ten (10) Business Days after your verbal notification. CREDIT UNION will tell you the results of our investigation within ten (10) Business Days after we hear from you and will correct any error promptly. However, if the CREDIT UNION requires more time to confirm the nature of your complaint or question, CREDIT UNION reserves the right to take up to forty-five (45) days to complete the investigation. If CREDIT UNION decides to do this, CREDIT UNION will provisionally credit your Payment Account within ten (10) Business Days for the amount you think is in error. If CREDIT UNION asks you to submit your complaint or question in writing and we do not receive it within ten (10) Business Days, CREDIT UNION may not provisionally credit your Payment Account. If it is determined there was no error, CREDIT UNION will mail you a written explanation within three (3) Business Days after completion of our investigation. You may ask for copies of documents used in CREDIT UNION'S investigation. The Service may revoke any provisional credit provided to you if CREDIT UNION find an error did not occur.

### **Disclosure of Account Information to Third Parties**

**32.** It is our general policy to treat your account information as confidential. However, CREDIT UNION will disclose information to third parties about your account or the transactions you make ONLY in the following situations:

- Where it is necessary for completing transactions;
- Where it is necessary for activating additional services;
- In order to verify the existence and condition of your account to a third party, such as a credit bureau or Biller;
- To a consumer reporting agency for research purposes only;

- In order to comply with a governmental agency or court orders;
- If you give us your written permission; or
- In accordance with the CREDIT UNION'S privacy policy.

### **Alterations and Amendments**

- 33.** This Agreement, applicable fees, and service charges may be altered or amended by the Service from time to time. In such event, the Service shall provide notice to you. Any use of the Service after the Service provides you a notice of change will constitute your agreement to such change(s). Further, the Service may, from time to time, revise or update the applications, services, and/or related material, which may render all such prior versions obsolete. Consequently, the Service reserves the right to terminate this Agreement as to all such prior versions of the applications, services, and/or related material and limit access to only the Service's more recent revisions and updates. In addition, as a part of this Service, you agree to receive all legally required notifications via electronic means.
- 34.** It is your sole responsibility to ensure that your contact information with the CREDIT UNION is current and accurate. This includes, but is not limited to, name, address, phone numbers, and email addresses. Changes can be made within the service using the "Update My Personal Profile" feature or by contacting the CREDIT UNION. Any changes in your Payment Account should also be made in accordance with the procedures outlined within Service online features. All changes made are effective immediately for scheduled and future payments paid from the updated Payment Account information. The Service is not responsible for any payment processing errors or fees incurred if you do not provide accurate Payment Account or contact information.
- 35.** CREDIT UNION or the Service may terminate or suspend Bill Pay Service to you at any time. Neither termination nor suspension shall affect your liability or obligations under this Agreement.

Any payment(s) the Service has already processed before the termination or suspension date will be completed by the Service. All Scheduled Payments (including, recurring payments) will not be processed once the Service is terminated or suspended.

### **Biller Limitation**



- 36.** The Service reserves the right to refuse to pay any Biller to whom you may direct a payment. The Service will notify you promptly if it decides to refuse to pay a Biller designated by you. This notification is not required if you attempt to make a prohibited payment or an exception payment under this Agreement.

### **Returned Payments**

- 37.** In using the Service, you understand that Billers and/or the United States Postal Service may return payments to the Service for various reasons such as, but not limited to, Biller's forwarding address expired; Biller account number is not valid; Biller is unable to locate account; or Biller account is paid in full. The Service will use its best efforts to research and correct the returned payment and return it to your Biller, or void the payment and credit your Payment Account. You may receive notification from the Service.

### **Information Authorization**

- 38.** Your enrollment in the Service may not be fulfilled if the service cannot verify your identity or other necessary information. In order to verify ownership of the Payment Account(s) and/or Billing Account, the Service may issue offsetting debits and credits to the Payment Account(s) and/or Billing Account, and require confirmation of such from you. Through your enrollment in the Service, you agree that the Service reserves the right to request a review of your credit rating at its own expense through an authorized bureau. In addition, you agree that the Service reserves the right to obtain financial information regarding your account from a Biller or your financial institution (for example, to resolve payment posting problems or for verification).

### **Disputes**

- 39.** In the event of a dispute regarding the Service, you and the Service agree to resolve the dispute by looking to this Agreement. You agree that this Agreement is the complete and exclusive statement of the agreement between you and the Service, which supersedes any proposal or prior agreement, oral or written, and any other communications between you and the Service relating to the subject matter of this Agreement. If there is a conflict between what an employee of the Service or Bill Pay Customer Care says and the terms of this Agreement, the terms of this Agreement will prevail.

### **Exclusion of Warranties**

**40.** THE SITE AND SERVICE AND RELATED DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN PARTICULAR, WE DO NOT GUARANTEE CONTINUOUS, UNINTERRUPTED OR SECURE ACCESS TO ANY PART OF OUR SERVICE, AND OPERATION OF OUR SITE MAY BE INTERFERED WITH BY NUMEROUS FACTORS OUTSIDE OF OUR CONTROL. SOME STATES DO NOT ALLOW THE DISCLAIMER OF CERTAIN IMPLIED WARRANTIES, SO THE FOREGOING DISCLAIMERS MAY NOT APPLY TO YOU. THIS PARAGRAPH GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

### **Limitation of Liability**

**41.** THE FOREGOING SHALL CONSTITUTE YOUR EXCLUSIVE REMEDIES AND THE ENTIRE LIABILITY OF US AND OUR AFFILIATES AND SERVICE PROVIDERS AND THE EMPLOYEES AND CONTRACTORS OF EACH OF THESE, FOR THE SERVICE AND THE PORTION OF THE SITE THROUGH WHICH THE SERVICE IS OFFERED. YOU ACKNOWLEDGE AND AGREE THAT FROM TIME TO TIME, THE SERVICE MAY BE DELAYED, INTERRUPTED OR DISRUPTED PERIODICALLY FOR AN INDETERMINATE AMOUNT OF TIME DUE TO CIRCUMSTANCES BEYOND OUR REASONABLE CONTROL, INCLUDING BUT NOT LIMITED TO ANY INTERRUPTION, DISRUPTION OR FAILURE IN THE PROVISION OF THE SERVICE, WHETHER CAUSED BY STRIKES, POWER FAILURES, EQUIPMENT MALFUNCTIONS, INTERNET DISRUPTION OR OTHER REASONS. IN NO EVENT SHALL WE OR OUR AFFILIATES OR SERVICE PROVIDERS, OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY CLAIM ARISING FROM OR RELATED TO THE SERVICE CAUSED BY OR ARISING OUT OF ANY SUCH DELAY, INTERRUPTION, DISRUPTION OR SIMILAR FAILURE. IN NO EVENT SHALL WE OR OUR AFFILIATES OR SERVICE PROVIDERS, OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING LOSS OF GOODWILL OR LOST PROFITS (EVEN IF ADVISED OF THE POSSIBILITY THEREOF) ARISING IN ANY WAY OUT OF THE INSTALLATION, USE OR MAINTENANCE OF THE SERVICE OR THE PORTION OF THE SITE THROUGH WHICH THE SERVICE IS OFFERED, EVEN IF SUCH DAMAGES WERE REASONABLY FORESEEABLE AND

NOTICE WAS GIVEN REGARDING THEM. IN NO EVENT SHALL WE OR OUR AFFILIATES OR SERVICE PROVIDERS, OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY CLAIM ARISING FROM OR RELATED TO THE SERVICE OR THE PORTION OF THE SITE THROUGH WHICH THE SERVICE IS OFFERED THAT YOU DO NOT STATE IN WRITING IN A COMPLAINT FILED IN A COURT OR ARBITRATION PROCEEDING AS DESCRIBED IN SECTIONS 37 AND 38 ABOVE WITHIN TWO (2) YEARS OF THE DATE THAT THE EVENT GIVING RISE TO THE CLAIM OCCURRED. THESE LIMITATIONS WILL APPLY TO ALL CAUSES OF ACTION, WHETHER ARISING FROM BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL THEORY. OUR AGGREGATE LIABILITY, AND THE AGGREGATE LIABILITY OF OUR AFFILIATES AND SERVICE PROVIDERS, AND THE EMPLOYEES AND CONTRACTORS OF EACH OF THESE, TO YOU AND ANY THIRD PARTY FOR ANY AND ALL CLAIMS OR OBLIGATIONS RELATING TO THIS AGREEMENT SHALL BE LIMITED TO DIRECT OUT OF POCKET DAMAGES UP TO A MAXIMUM OF \$500 (FIVE HUNDRED DOLLARS). SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

### **Miscellaneous**

- 42.** You may not assign this Agreement to any other party. The Service may assign this Agreement to any future, directly or indirectly, affiliated company. The Service may also assign or delegate some of its rights and responsibilities under this Agreement to independent contractors or other third parties.
- 43.** The Service shall not be deemed to have waived any of its rights or remedies hereunder unless such waiver is in writing and signed by the Service. No delay or omission on the part of the Service in exercising any rights or remedies shall operate as a waiver of such rights or remedies or any other rights or remedies. A waiver on any one occasion shall not be construed as a bar or waiver of any rights or remedies on future occasions.
- 44.** 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.
- 45.** This Agreement shall be governed by and construed in accordance with the laws of the State where CREDIT UNION is Chartered, without regard to its conflicts of laws provisions. To the extent that the terms of this Agreement

conflict with applicable state or federal law, such state or federal law shall replace such conflicting terms only to the extent required by law. Unless expressly stated otherwise, all other terms of this Agreement shall remain in full force and effect.

46. CREDIT UNION and the Service will provide your Bill Pay Terms and Conditions Agreement electronically. This Agreement will remain available online for you to print. the CREDIT UNION will also provide notices of changes to this Agreement and other related disclosures, if required by law, electronically through the Service's e-messaging system, or U.S. mail to the CREDIT UNION'S address of record. In addition, the CREDIT UNION' will provide changes to the terms of this Electronic Disclosures Agreement and other related disclosures electronically.
47. You agree that this Agreement is the complete and exclusive statement of the agreement between you and the CREDIT UNION, sets forth the entire understanding between us 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.

**\*\*\* The Following Sections Only Apply to Users of the  
IPAY BILL PAY SYSTEM \*\*\***

**iPay Bill Pay Terms and Conditions**

**Definitions**

"Agreement" means these Terms and Conditions of the CREDIT UNION Bill Pay Service.

"Biller" is the person or entity to which you wish a bill payment to be directed or is the person or entity from which you receive electronic bills (E-Bills), as the case may be.

"Business Day" is every Monday through Friday, Eastern Time, excluding Federal Reserve holidays.

"External Transfers" means when you transfer funds out of your CREDIT UNION account for credit to an external account at another financial institution.

"Payment Instruction" is the information provided by you to the Service for a bill payment to be made to the Biller (such as, but not limited to, Biller name, Biller account number, and Scheduled Payment Date).

"Payment Account" is the checking account from which bill payments will be debited.

"Scheduled Payment" is a payment that has been scheduled through the Service but has not begun processing.

"Service" means the Bill Pay Service offered by the CREDIT UNION, through our designated service provider.

"Service Provider" means companies that we have engaged to render some or all of the Service to you on our behalf.

**Transfers**

There is no limit on the number of transfers from your savings account or your Money Market Savings Account if they are made in person, by Automatic Teller, or by mail, or if they are made to make monthly payments on the CREDIT UNION loans, to have funds mailed directly to you, or as a distribution of your Direct Deposit.

Federal regulations limit the number of certain types of transfers and/or withdrawals you can make from your savings account and your Money Market Savings Account to six per calendar month. The types of transfers that are limited are those requested by fax, telephone, internet, and pre-authorized transfers.

## **Liability for Failure to Make Transfers**

If the CREDIT UNION does not complete a transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will NOT be liable, for instance, if, through no fault of ours:

- you do not have sufficient funds in your account or available credit in your line of credit to make the transfer;
- someone to whom you have provided your account information and PIN makes a transfer;
- your bill payment request contains an error or is a duplicate of another bill payment;
- if the funds in your account are subject to legal process, such as garnishment or attachment; if the account is subject to a pledge or security agreement;
- or if, despite reasonable precautions that we have taken, circumstances beyond our control (such as fire, power failure, flood, or failure of paying agency to deliver direct deposit payment data) prevent the transfer.

## **Account Information Disclosure**

We will disclose information to third parties about your account or the transactions you make:

- If we return checks on your account drawn on non-sufficient funds or if we are unable to complete an electronic transfer because of non-sufficient funds.
- When it is necessary for completing transfers.
- To verify the existence or conditions of your account for a third party, such as a credit bureau or merchant.

- To comply with government agency or court orders.
- If you give us your written permission.
- In accordance with our privacy policy.

### **Failed or Returned Transactions**

In using the Service, you are requesting the Service to make payments for you from your Payment Account. If we are unable to complete the transaction for any reason associated with your Payment Account (for example, there are non-sufficient funds in your Payment Account to cover the transaction), the transaction will not be completed. In some instances, you will receive a return notice from the Service. In such case, you agree that:

- You will reimburse the Service immediately upon demand the transaction amount that has been returned to the Service;
- For any amount not reimbursed to the Service within fifteen (15) days of the initial notification, a late charge equal to 1.5% monthly interest or the legal maximum, whichever rate is lower, for any unpaid amounts may be imposed;
- You will reimburse the Service for any fees imposed by your financial institution as a result of the return;
- You will reimburse the Service for any fees it incurs in attempting to collect the amount of the return from you; and
- The Service is authorized to report the facts concerning the return to any consumer credit reporting agency.

In these cases, you agree that a non-sufficient funds (NSF) fee will be charged in accordance with the CREDIT UNION'S published fees. Further, you also agree that a NSF fee may be charged to your account even if the payment is not returned but is paid and overdraws your Payment Account.

### **Bill Payment Scheduling**

The earliest possible payment for each Biller (typically five [5] or fewer Business Days from the current date) will be designated within the application when you are scheduling the payment. Therefore, the application will not permit you to select a date less than the earliest possible date designated for each Biller. When scheduling payments, select a date that allows adequate time for delivery prior to any late date or grace period. For External Transfers the account debit will take place on the day the External Transfer is sent.

## Prohibited Payments

The following types of payments are prohibited through the Service, and we have the right but not the obligation to monitor for, block cancel and/or reverse such payments:

Payments to persons or entities located in prohibited territories (including any territory outside of the United States); Payments that violate any law, statute, ordinance or regulation; Payments related to: (1) tobacco products, (2) prescription drugs and devices; (3) narcotics, steroids, controlled substances or other products that present a risk to consumer safety; (4) drug paraphernalia; (5) ammunition, firearms, or firearm parts or related accessories; (6) weapons or knives regulated under applicable law; (7) goods or services that encourage, promote, facilitate or instruct others to engage in illegal activity; (8) goods or services that are sexually oriented; (9) goods or services that promote hate, violence, racial intolerance, or the financial exploitation of a crime; (10) goods or services that defame, abuse, harass or threaten others; (11) goods or services that include any language or images that are bigoted, hateful, racially offensive, vulgar, obscene, indecent or discourteous; (12) goods or services that advertise or sell to, or solicit others; or (13) goods or services that infringe or violate any copyright, trademark, right of publicity or privacy or any other proprietary right under the laws of any jurisdiction; Payments related to gambling, gaming and/or any activity with an entry fee and a prize, including, but not limited to casino games, sports betting, horse or greyhound racing, lottery tickets, other ventures that facilitate gambling, games of skill (whether or not it is legally defined as a lottery) and sweepstakes; Payments relating to transactions that (1) support pyramid or Ponzi schemes, matrix programs, other "get rich quick" schemes or multi-level marketing programs, (2) are associated with purchases of real property, annuities or lottery contracts, lay-away systems, off-shore banking or transactions to finance or refinance debts funded by a credit card, (3) are for the sale of items before the seller has control or possession of the item, (4) constitute money-laundering or terrorist financing; (5) are associated with the following "money service business" activities: the sale of traveler's checks or money orders, currency dealers or exchanges or check cashing, or (6) provide credit repair or debt settlement services; Tax payments and court ordered payments including but not limited to Alimony and Child Support.

In no event shall we or our independent contractors or other third parties to whom we assign or delegate rights or responsibilities be liable for any claims or damages resulting from your scheduling of prohibited payments. We have no obligation to research or resolve any claim resulting from a prohibited payment. All research and resolution for any misapplied, mis-posted or misdirected prohibited payments will be your sole responsibility and not ours.



We encourage you to provide notice to us by the methods described in above of any violations of this section or the Agreement generally.

## **Payment Authorization and Payment Remittance**

By providing the Service with names and account information of Billers to whom you wish to direct payments, you authorize the Service to follow the Payment Instructions that it receives through the payment system. In order to process payments more efficiently and effectively, the Service may edit or alter payment data or data formats in accordance with Biller directives.

When the Service receives a Payment Instruction, you authorize the Service to debit your Payment Account and remit funds on your behalf so that the funds arrive as close as reasonably possible to the Scheduled Payment Date designated by you. You also authorize the Service to credit your Payment Account for payments returned to the Service by the United States Postal Service or Biller, or payments remitted to you on behalf of another authorized user of the Service.

The Service will use its best efforts to make all your payments properly. However, the Service shall incur no liability, and any Service Guarantee shall be void if the Service is unable to complete any payments initiated by you because of the existence of any one or more of the following circumstances:

- If, through no fault of the Service, your Payment Account does not contain sufficient funds to complete the transaction or the transaction would exceed the credit limit of your line of credit account. Per federal regulation, pre-authorized telephone, Internet, or automatic transfers from savings to cover checking overdrafts cannot exceed six (6) in number per calendar month;
- The payment processing center is not working properly, and you know or have been advised by the Service about the malfunction before you execute the transaction;
- You have not provided the Service with the correct Payment Account Information, or the correct name, address, phone number, or account information for the Biller; and/or
- Circumstances beyond control of the Service (such as, but not limited to, fire, flood, or interference from an outside force) prevent the proper execution of the transaction, and the Service has taken reasonable precautions to avoid those circumstances.

Provided none of the foregoing exceptions are applicable, if the Service causes an incorrect amount of funds to be removed from your Payment

Account or causes funds from your Payment Account to be directed to a Biller that does not comply with your Payment Instructions, the Service shall be responsible for returning the improperly transferred funds to your Payment Account, directing to the proper Biller any previously misdirected transactions, and, if applicable, any late payment-related charges.

The Service reserves the right to select the method in which to remit funds on your behalf to your Biller. These payment methods may include, but may not be limited to, an electronic payment or a laser draft payment (funds remitted to the Biller are deducted from your Payment Account when the laser draft is presented to your financial institution for payment).

### **Payment Cancellation Requests**

You may cancel or edit any Scheduled Payment (including recurring payments) by following the directions within the application. There is no charge for canceling or editing a Scheduled Payment. Once the Service has begun processing a payment, it cannot be canceled or edited. Therefore, a stop payment request must be submitted.

The Service's ability to process a stop payment request will depend on the payment method and whether or not a check has cleared. The Service may also not have a reasonable opportunity to act on any stop payment request after a payment has been processed. If you desire to stop any payment that has already been processed, you must contact Bill Pay Customer Care, offered through our Service Provider. Although the Service will make every effort to accommodate your request, the Service will have no liability for failing to do so. The Service may also require you to present your request in writing within fourteen (14) days. Please refer to the CREDIT UNION'S fees, which can be found on the CREDIT UNION website.

### **Electronic Bill (E-Bill) Delivery and Presentment**

This feature is for the presentment of electronic bills (E-Bills) only, and it is your sole responsibility to contact your Billers directly if you do not receive your statements. In addition, if you elect to activate one of the Service's electronic bill options, you also agree to the following:

- Information provided to the Biller – The Service is unable to update or change your personal information such as, but not limited to, name, address, phone numbers, and email addresses with the electronic Biller. Any changes will need to be made by contacting the Biller directly. Additionally, it is your responsibility to maintain all usernames and passwords for all electronic Biller sites. You also agree not to use someone else's information to gain unauthorized access to another person's bill. The Service may, at the request of the Biller,

provide to Biller your email address, service address, or other data specifically requested by the Biller at the time of activating the electronic bill for that Biller, for the purposes of the Biller informing you about Service and/or bill information.

- Activation – Upon activation of the electronic bill feature, the Service may notify the Biller of your request to receive electronic billing information. The presentment of your first electronic bill may vary from Biller to Biller and may take up to sixty (60) days, depending on the billing cycle of each Biller. Additionally, the ability to receive a paper copy of your statement(s) is at the sole discretion of the Biller. While your electronic bill feature is being activated, it is your responsibility to keep your accounts current. Each electronic Biller reserves the right to accept or deny your request to receive electronic bills.
- Authorization to obtain bill data – Your activation of the electronic bill feature for a Biller shall be deemed by us to be your authorization for us to obtain bill data from the Biller on your behalf. For some Billers, you will be asked to provide us with your username and password for that Biller. By providing us with such information, you authorize us to use the information to obtain your bill data.
- Notification – The Service will use its best efforts to present all of your electronic bills promptly. In addition to notification with the Service, the Service may send an email notification to the email address listed for your account. It is your sole responsibility to ensure that this information is accurate. In the event you do not receive notification, it is your responsibility to periodically log in to the Service and check on the delivery of new electronic bills. The time for notification may vary from Biller to Biller. You are responsible for ensuring timely payment of all bills.
- Cancellation of electronic bill notification – The electronic Biller reserves the right to cancel the presentment of electronic bills at any time. You may cancel electronic bill presentment at any time. The timeframe for cancellation of your electronic bill presentment may vary from Biller to Biller. It may take up to sixty (60) days, depending on the billing cycle of each Biller. The Service will notify your electronic Biller(s) as to the change in status of your account, and it is your sole responsibility to make arrangements for an alternative form of bill delivery. The Service will not be responsible for presenting any electronic bills that are already in process at the time of cancellation.

- Non-delivery of electronic bill(s) – You agree to hold the Service harmless should the Biller fail to deliver your statement(s). You are responsible for ensuring timely payment of all bills. Copies of previously delivered bills must be requested from the Biller directly.
- Accuracy and dispute of electronic bill – The Service is not responsible for the accuracy of your electronic bill(s). The Service is only responsible for presenting the information we receive from the Biller. Any discrepancies or disputes regarding the accuracy of your electronic bill summary or detail must be addressed with the Biller directly.

This Agreement does not alter your liability or obligations that currently exist between you and your Billers.

### **Biller Limitations**

The Service reserves the right to refuse to pay any Biller to whom you may direct a payment. The Service will notify you promptly if it decides to refuse to pay a Biller designated by you. This notification is not required if you attempt to make a prohibited payment or an exception payment under this Agreement.

### **Returned Payments**

In using the Service, you understand that Billers and/or the United States Postal Service may return payments to the Service for various reasons such as, but not limited to, Biller's forwarding address expired; Biller account number is not valid; Biller is unable to locate account; or Biller account is paid in full. The Service will use its best efforts to research and correct the returned payment and return it to your Biller, or void the payment and credit your Payment Account. You may receive notification from the Service.

### **Information Authorization**

Your enrollment in the Service may not be fulfilled if the service cannot verify your identity or other necessary information. In addition, you agree that the Service reserves the right to obtain financial information regarding your account from a Biller or your financial institution (for example, to resolve payment posting problems or for verification)

### **Amendment of this Agreement**

We may amend the terms of this Agreement by giving you notice of the amendment. Your continued use of the Service after such notice is given constitutes your agreement to the amendments.

## **Exclusion of Warranties**

THE SITE AND SERVICE AND RELATED DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN PARTICULAR, WE DO NOT GUARANTEE CONTINUOUS, UNINTERRUPTED OR SECURE ACCESS TO ANY PART OF OUR SERVICE, AND OPERATION OF OUR SITE MAY BE INTERFERED WITH BY NUMEROUS FACTORS OUTSIDE OF OUR CONTROL. SOME STATES DO NOT ALLOW THE DISCLAIMER OF CERTAIN IMPLIED WARRANTIES, SO THE FOREGOING DISCLAIMERS MAY NOT APPLY TO YOU. THIS PARAGRAPH GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

## **Limitation of Liability**

THE FOREGOING SHALL CONSTITUTE YOUR EXCLUSIVE REMEDIES AND THE ENTIRE LIABILITY OF US AND OUR AFFILIATES AND SERVICE PROVIDERS AND THE EMPLOYEES AND CONTRACTORS OF EACH OF THESE, FOR THE SERVICE AND THE PORTION OF THE SITE THROUGH WHICH THE SERVICE IS OFFERED. YOU ACKNOWLEDGE AND AGREE THAT FROM TIME TO TIME, THE SERVICE MAY BE DELAYED, INTERRUPTED OR DISRUPTED PERIODICALLY FOR AN INDETERMINATE AMOUNT OF TIME DUE TO CIRCUMSTANCES BEYOND OUR REASONABLE CONTROL, INCLUDING BUT NOT LIMITED TO ANY INTERRUPTION, DISRUPTION OR FAILURE IN THE PROVISION OF THE SERVICE, WHETHER CAUSED BY STRIKES, POWER FAILURES, EQUIPMENT MALFUNCTIONS, INTERNET DISRUPTION OR OTHER REASONS. IN NO EVENT SHALL WE OR OUR AFFILIATES OR SERVICE PROVIDERS, OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY CLAIM ARISING FROM OR RELATED TO THE SERVICE CAUSED BY OR ARISING OUT OF ANY SUCH DELAY, INTERRUPTION, DISRUPTION OR SIMILAR FAILURE. IN NO EVENT SHALL WE OR OUR AFFILIATES OR SERVICE PROVIDERS, OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING LOSS OF GOODWILL OR LOST PROFITS (EVEN IF ADVISED OF THE POSSIBILITY THEREOF) ARISING IN ANY WAY OUT OF THE INSTALLATION, USE OR MAINTENANCE OF THE SERVICE OR THE PORTION OF THE SITE THROUGH WHICH THE SERVICE IS OFFERED, EVEN IF SUCH DAMAGES WERE

REASONABLY FORESEEABLE AND NOTICE WAS GIVEN REGARDING THEM. IN NO EVENT SHALL WE OR OUR AFFILIATES OR SERVICE PROVIDERS, OR THE EMPLOYEES OR CONTRACTORS OF ANY OF THESE, BE LIABLE FOR ANY CLAIM ARISING FROM OR RELATED TO THE SERVICE OR THE PORTION OF THE SITE THROUGH WHICH THE SERVICE IS OFFERED THAT YOU DO NOT STATE IN WRITING IN A COMPLAINT FILED IN A COURT OR ARBITRATION PROCEEDING WITHIN TWO (2) YEARS OF THE DATE THAT THE EVENT GIVING RISE TO THE CLAIM OCCURRED. THESE LIMITATIONS WILL APPLY TO ALL CAUSES OF ACTION, WHETHER ARISING FROM BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL THEORY. OUR AGGREGATE LIABILITY, AND THE AGGREGATE LIABILITY OF OUR AFFILIATES AND SERVICE PROVIDERS, AND THE EMPLOYEES AND CONTRACTORS OF EACH OF THESE, TO YOU AND ANY THIRD PARTY FOR ANY AND ALL CLAIMS OR OBLIGATIONS RELATING TO THIS AGREEMENT SHALL BE LIMITED TO DIRECT OUT OF POCKET DAMAGES UP TO A MAXIMUM OF \$500 (FIVE HUNDRED DOLLARS). SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.