
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 and 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
PASSWORD / USERNAME/ACTIVATION DECISIONS TO MAKE	12
CONTROLLING ACTIVATION SETTINGS	17
TO ACTIVATE OR NOT TO ACTIVATE?	17
NEW MEMBER ACCESS CONTROLS	17
ACTIVATE/DEACTIVATE VIA MEMBER PERSONAL BANKER	17
"TRY IT BEFORE YOU BUY IT!" – PROMOTIONAL CAMPAIGNS	18
CONFIGURING A PROMOTIONAL CAMPAIGN	19
MESSAGING ON ENTRY EXPLAINS REASON MEMBER NEEDS RESET	23
INCORRECT PASSWORD ENTRIES RESET	23
RESET FOR THREE INCORRECT SECURITY QUESTION ANSWERS	24

Revision date: February 7, 2017

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.

RESET PASSWORD EXPIRED DUE TO NON-USE	26
<u>USERNAMES</u>	<u>27</u>
OPTIONAL USERNAME	27
REQUIRED USERNAMES	28
ASSISTING A MEMBER WITH A USERNAME IN CU*BASE	29
<u>ESTATEMENT SECURITY</u>	<u>31</u>
ONLINE BANKING INDEMNIFICATION NOT REQUIRED FOR eSTATEMENTS	31
UN-ENROLLING A BATCH OF MEMBERS	31
<u>OPTIONAL FEATURES MEMBERS USE TO SECURE ACCESS</u>	<u>32</u>
HIDE MY TYPING	32
PASSWORD STRENGTH EDUCATION TOOL	32
<u>TIMEOUT NOTIFICATION</u>	<u>33</u>
<u>PASSWORD CHANGE REMINDERS</u>	<u>34</u>
<u>PERSONAL INFORMATION CHANGE NOTIFICATIONS</u>	<u>35</u>
CHANGES TO ONLINE BANKING PASSWORD AND EMAIL	35
PERSONAL INFORMATION CHANGES	36
RED FLAG WARNINGS IN CU*BASE FOR EMPLOYEES	36
<u>SEE/JUMP ACCESS CONTROLS</u>	<u>38</u>
<u>INTER-MEMBER TRANSFER CONTROLS</u>	<u>39</u>
OVERVIEW	39
TRANSFER CONTROL LISTS	39
DIRECT ACCOUNT INPUT	39
INTER-MEMBER TRANSFERS: WHAT THE MEMBER SEES IN ONLINE BANKING	40
<u>EVALUATING THE REASON FOR A PASSWORD CHANGE</u>	<u>41</u>
<u>EVALUATING YOUR MEMBERSHIPS WITHOUT ACTIVITY</u>	<u>42</u>
REVIEW YOUR CREDIT UNION PLAN AND PROCEDURES	42
<u>APPENDIX A: ONLINE BANKING USE AGREEMENT</u>	<u>44</u>

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 128-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 VeriSign digital certification (www.verisign.com), 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 27** 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.

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.

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 Internet Explorer (PC) and Safari (on a MAC).
- The browser must have session cookies and JavaScript enabled.
- The browser must use 128-bit encryption. (To check the encryption level, from the Help menu, choose Help About... and look for a cipher strength or "high-grade security" notation indicating 128-bit strength.)
- Current usage requirements are available to members via **It's Me 247** online help  **HELP**.

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 **Update ARU/Online Banking Access** on the Update Functions 2 (MNUPDA) menu or through **Member Personal Banker** on the Member Service (MNSERV) menu.

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 (PCMBRCFG) 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 the **Member Personal Banker** on the Member Service (MNSERV) menu, he or she will see a messaging window (see page 23) 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 **Update ARU/Online Banking Access** on the Update Functions 2 (MNUPDA) menu

Expired Due to Non-Use - Refers to when a member has not used **It's Me 247** for a period of time, determined by the expiration period (in days) in the credit union's ARU/Online Banking configuration. 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 **Member Personal Banker** (accessed on the Member Service (MNSERV) menu), the MSR will receive messaging (see page 23) 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 **Update ARU/Online Banking Access** on the Update Functions 2 (MNUPDA) menu. 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 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 39 for more information.

Password Strength Educational Tool – Members can use this tool to gauge the strength of their new password when updating or changing their password in **It's Me 247**.

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 18) 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.

See/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 either “Jump” to another account (for almost full permissions) or remain in their original account and “See” account balance and transaction information for their other accounts. See page 38 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.

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 due to the fact that 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

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 39 for more information.

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. Usernames can be a maximum of twenty characters. Refer to Page 3 for rules when creating usernames. Refer to Page 27 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 **10 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)
- ◆ 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)

NOTE: Certain special characters are not allowed due to the fact that 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. Refer to Page 3 for rules when creating usernames. Refer to Page 27 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.
- ◆ Members can request at any time that the credit union reset their password, for example, they may need a reset after entering the wrong password three times or entering their security questions incorrectly three times. **After following credit union policy, the member service representative can reset the password** using **Member Personal Banker** on the Member Service (MNSERV) menu. 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. (This configuration is set by the credit union via the Internet Member Services Config (MNCNFE) menu.) 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.
- ◆ **Online banking passwords can be configured to expire after a certain period of non-use.** Enter a configured number of days (1-90) in the credit union ARU/Online Banking configuration in OPER. (Or the credit union can select 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 expiration comes into play only after a member has not logged into **It's Me 247** for a certain period of time. 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 the ARU/Online Banking configuration in OPER, 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 of time. Refer to page 18 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.

PASSWORD / USERNAME/ACTIVATION

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 of the bases. If you would like to make any changes to 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).

- **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>
Activation Settings		
What should the temporary password setting be for the credit union?	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 period, or promotional campaign). Credit unions have four configurations to select from for their temporary password, including: <ul style="list-style-type: none"> • Last four digits of SSN (current option) • First four digits of SSN and last two letters of last name (all CAPS) • Birth year and first two letters of last name (all CAPS) • Last four digits of SSN and birth year 	Contact Client Services to change the temporary password setting
Should usernames be required?	Your credit union can elect to require usernames be used in place of account numbers when logging into online banking. <ul style="list-style-type: none"> • 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 logging into online banking use their username in place of the account number. • Members create usernames in online banking. Usernames can be viewed and deleted in CU*BASE, but cannot be added for the member. • Refer to Page 3 for rules when creating usernames. • Refer to Page 27 for more information about usernames. 	For newly converting credit unions, talk to your Conversion Coordinator about the desired setting when your credit union switches to CU*BASE and It's Me 247 . For existing clients, contact Client Services to activate this feature, if your credit union elects to do so.

<p>Should all existing memberships be activated automatically?</p>	<ul style="list-style-type: none"> 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). <p>IMPORTANT: 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 It's Me 247 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.</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 It's Me 247</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>
<p>Should <u>new</u> members automatically be granted access and given a password?</p>	<ul style="list-style-type: none"> Configure whether or not to activate online banking automatically for new memberships If all new members are granted access, the number of days a new member password is active is configurable. See the Password section. 	<p>Contact Client Services to change the activation setting for new memberships. (Days for password to be active are controlled by the credit union.)</p>
<p>If members are not automatically be activated, how do they become activated?</p>	<ul style="list-style-type: none"> Develop an internal policy and procedure MSRs and phone staff can use to sell online banking and activate the new member's account 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 It's Me 247 until requested <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>	<p>Use Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu to activate a member's account</p>
<p>What if a member misuses the system or requests that no access be allowed to his accounts via online banking?</p>	<ul style="list-style-type: none"> Any member account can be permanently disabled from either online banking or audio response, or both 	<p>Use Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu and change the activation flag to disable an account</p>

Passwords

<p>Do you want to force complex password rules?</p>	<ul style="list-style-type: none"> • Activate the complex passwords flag 	<p>Contact Client Services for configuration</p>
<p>What should your expiration period be for members who do <u>not</u> use It's Me 247 regularly?</p>	<ul style="list-style-type: none"> • Configure expiration period by number of days (1-90 days, for example 60 days). (Select 999 for never to expire.) • If expired member tries to log in, will be notified as follows: 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. • 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. 	<p>Contact Client Services to configure the expiration period (for non-use)</p> <p>To reset an expired member's password to the temporary password the MSR will use Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu</p>
<p>Would you like to activate all members to start, but then "close" the enrollment period after a period of 1-7 days?</p>	<ul style="list-style-type: none"> • Check to activate all online banking enrollments; also activate all new memberships automatically • Credit unions can select to have a new member temporary password be valid for one to seven days (seven being the default). • 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). 	<p>Use Online Banking VMS Configuration on the Internet Member Services Config menu (MNCNFE) to configure the number of days the password until the password is expired.</p> <p>To allow a member in after the period, the MSR must <u>reset</u> the password using Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu</p>
<p>Do you want to market an open enrollment period on a regular basis?</p>	<ul style="list-style-type: none"> • 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) 	<p>Use Config New User Promo Campaign on the Internet Member Services Config (MNCNFE) menu</p>

Maintenance Tasks

<p>Do you want to allow your staff to set custom passwords for members who are having trouble setting their own?</p>	<ul style="list-style-type: none"> If not, you can choose to disable the custom password option for all memberships; MSR's must <u>reset</u> a password to the temporary password then instruct the member to change the password manually using It's Me 247 Develop an internal credit union policy and procedure for your staff 	<p>Contact Client Services to disable the custom password option. Or grant access to Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu only to staff that are authorized to set custom passwords</p>
<p>How will MSR's validate identity when a member calls to be reactivated after his/her password has expired?</p>	<ul style="list-style-type: none"> Develop an internal credit union policy and procedure for your staff 	<p>To allow a member in after the expiration period, the MSR must <u>reset</u> the password using Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu</p>
<p>What if a member loses his or her password?</p>	<ul style="list-style-type: none"> Develop an internal policy and procedure MSR's and phone staff should use to verify identity Reset the password to the configured credit union temporary password; the member will be required to change it immediately upon logging in <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>	<p>Use Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu to reset a password</p>
<p>What if a member knows his or her password but forgets the answers to his or her challenge questions?</p>	<ul style="list-style-type: none"> Develop an internal policy and procedure MSR's and phone staff should use to verify identity 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 <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>	<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.)</p>
<p>What if a member forgets his or her password and also forgets the answers to his or her challenge questions?</p>	<ul style="list-style-type: none"> Develop an internal policy and procedure MSR's and phone staff should use to verify identity. Reset the password to the configured credit union temporary password; the member will be required to change it immediately upon logging in 	<p>Use Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu to delete the member's questions and answers. A</p>

	<ul style="list-style-type: none"> • 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 • <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>confirmation will be required. This process will also reset the member’s password to the temporary password.</p>
<p>What if a member forgets his or her username?</p>	<ul style="list-style-type: none"> • 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. • Develop an internal policy and procedure MSRs and phone staff should use to verify identity. • Either view or delete the member’s username. NOTE: The employee will see the member’s username prior to deleting it. • Refer to Page 3 for rules when creating usernames. 	<p>Use Member Personal Banker on the Member Service (MNSERV) menu or Update Audio/Online Banking Access on the Update Functions 2 (MNUPDA) menu 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>

CONTROLLING ACTIVATION SETTINGS

Once you decide on basic password parameters, the next thing to think about is how you will control when and how a member is initially “activated” to be able to use **It’s Me 247** at all. Your credit union might just want to “flip the switch” to activate all members at the same time, but does your job end there? What about all of the members who will never even try **It’s Me 247**? Examiners are increasingly expressing concern over the risk of giving all members *carte blanche* access without any control or monitoring to ensure that only those members who really want to have ongoing access.

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.

NEW MEMBER ACCESS CONTROLS

If you select to active all members during enrollment, the “new member enrollment” expiration restricts this enrollment to a limited period of days - from one to seven days. This feature is controlled in the **Online Banking – VMS configuration** on the Internet Services Member Config (MNCNFE) menu. Credit unions can select a range with seven being the default. If the member does not login during this configured number of days, the member will be required to contact the credit union for a password reset.

of days a new member has to log in to online banking (1-7)

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 **Member Personal Banker** on the Member Services (MNSERV) menu, 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

The screenshot shows a web application window titled "Session 0 CU*BASE GOLD Edition - ABC TESTING CREDIT UNION". The main heading is "Update Audio/Online Banking Access" with an "UPDATE" button on the right. Below the heading, the account name "MARY MEMBER" is displayed. A status bar indicates "The Member is Allowed to Access This Account Using". There are two main sections: "Online banking" and "Audio response". Each section has a checked checkbox, a "Reason" dropdown menu set to "D02", and a search icon. Below these are two sections: "Change Password" and "Change PIN", each with a checkbox and a note: "Reset password to the last four digits of the member's SSN & the membe" and "Reset PIN to last four digits of member's SSN" respectively.

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.)

“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 **Config New User Promo Campaign** on the Internet Member Services Config (MNCNFE) menu. 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

CONFIGURING A PROMOTIONAL CAMPAIGN

“Config New User Promo Campaign” on the Internet Member Services Config (MNCNFE) menu

Session 0 CU*BASE GOLD Edition - Configure Online Banking Promotional Period

Corp ID 01

Set Up Online Banking Promotional Date

Description

Promotional period start date 00000000 [MMDDYYYY] for 000 days (Cannot be greater than 90)

Ending on 0/00/0000

Actv/View Members

Delete

BT (3656)

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)

Session 0 CU*BASE GOLD Edition - Configure Online Banking Promotional Period

Corp ID 01

Set Up Online Banking Promotional Date

Description AUGUST PROMOTION

Promotional period start date Aug 01, 2013 [MMDDYYYY] for 031 days (Cannot be greater than 90)

Ending on Sep 01, 2013

Actv/View Members

Delete

BT (3856)

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

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
93	OLETON	Oct 27, 2011	Sep 25, 2008	Feb 24, 2010	Y	N
85	PS	Nov 14, 2011	Jul 01, 1987	Jun 17, 2010	N	N
41	AND	Feb 23, 2009	Jul 01, 1987	0/00/0000	N	N
21	AND	Jul 23, 2012	Jul 25, 2008	Jul 19, 2010	N	N
31	ARLAND	Feb 24, 2011	Jul 25, 2008	Jul 19, 2010	N	N
41	LAND	Feb 24, 2011	Feb 24, 2011	0/00/0000	N	N
81	NER	0/00/0000	Jul 01, 1987	0/00/0000	N	N
21	NIX	0/00/0000	Jul 01, 1987	0/00/0000	N	N
01	?	0/00/0000	Jul 01, 1987	0/00/0000	Y	N
11	ATION	Jun 26, 2012	May 16, 1995	Mar 05, 2010	N	N
21	INTERNATIONAL ASSOC	Feb 20, 2009	May 16, 1995	Jan 16, 2009	N	N
81		Jan 02, 2007	May 17, 1995	Mar 05, 2003	N	N
11	ELL	Oct 02, 2012	May 18, 1995	Feb 15, 2010	N	N
21	SSIG	Nov 13, 2012	May 18, 1995	Feb 15, 2010	N	N
41		Jun 15, 2007	May 19, 1995	Jun 15, 2007	N	N
51	AR	Nov 14, 2011	May 19, 1995	Feb 16, 2010	N	N

Total number of members affected by promotional period 23,271

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

BT (3859) 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)

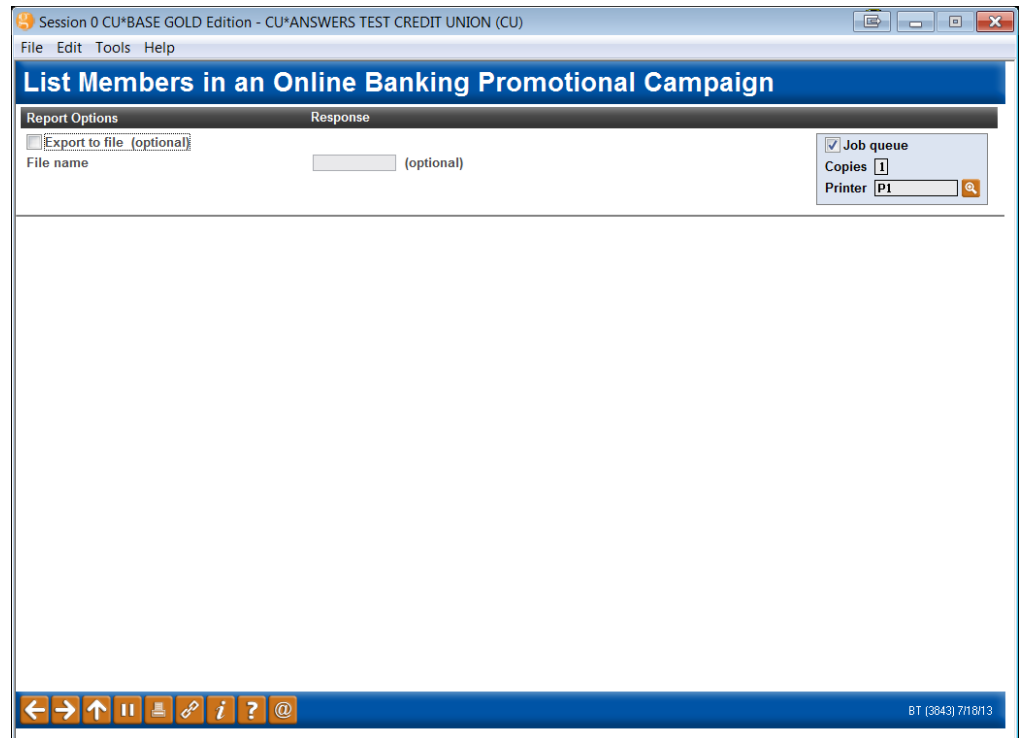
Use *Refresh* or press Enter to refresh your list to exclude (or include) members based on these selections.

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.

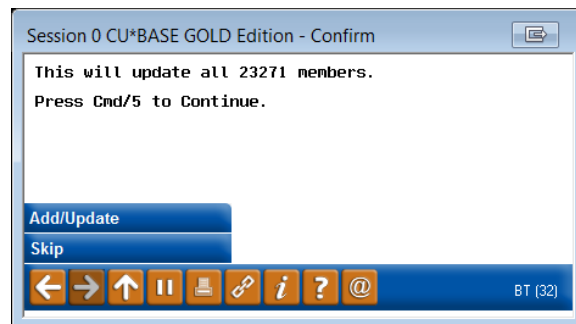
- NOTE: During a campaign, you can return to this screen to print updated results to a file for further analysis in Report Builder.

Print a Member File



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

Confirmation of Activation



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
2H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
5W		Feb 14, 2013	Dec 12, 1964	Mar 12, 2010	Y	N	
7H		0/00/0000	Dec 14, 1964	0/00/0000	N	N	
0H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
1W		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
0J		Dec 31, 2011	Dec 12, 1964	Nov 08, 2010	Y	N	
7C		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
1H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
2H		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
5N		Jun 08, 2011	Dec 12, 1964	Jun 08, 2011	N	N	
6C		May 10, 2010	Dec 12, 1964	Oct 25, 2002	N	N	
8W		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
1C		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
2C		0/00/0000	Dec 12, 1964	0/00/0000	N	N	
9F		Jul 05, 2006	Dec 12, 1964	Jul 05, 2006	N	N	
9W		0/00/0000	Dec 12, 1964	0/00/0000	N	N	

■ Select

Total number of members affected by promotional period 27,390

Total number of members who have logged in during promotional period 1

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

Print

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 particular member.

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

1. Select **Member Personal Banker** from the Member Service (MNSERV) menu.
2. Enter the members account number and press Enter
3. Select *Online banking/ARU (activate, change, PIN/Password; view password history* and press Enter.

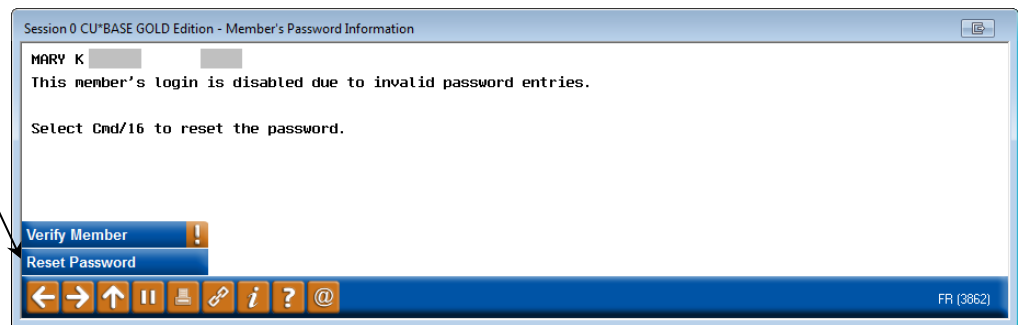
(These screens will also appear when you change a password via the Update Functions (MNUPDA) menu.)

These screens will appear even before you access the Update Audio/Online Banking Access screen (shown on page 24)

INCORRECT PASSWORD ENTRIES RESET

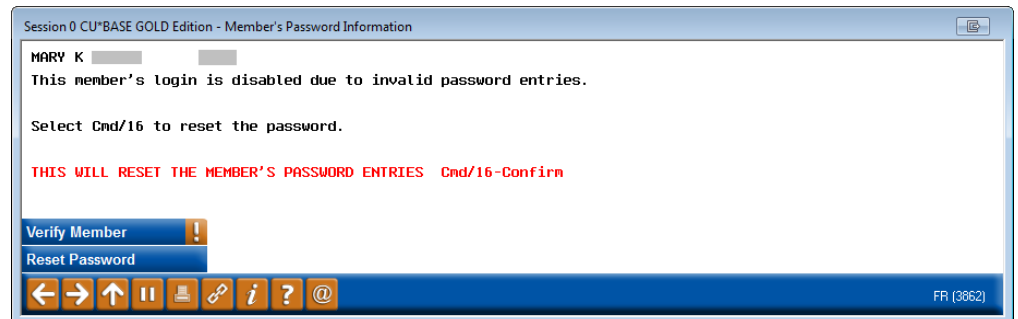
Members are locked out of their accounts after three incorrect password attempts. Following are the screens the MSR will see when assisting a member. After following the steps above, these three screens will walk the MSR through the password reset.

Explanation that Password Needs Reset Due to Invalid Password Tries



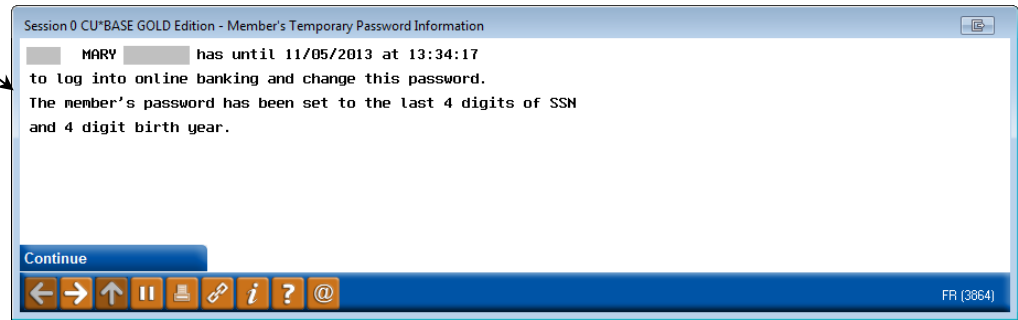
All entry explanatory screens have a *Verify Member* (F1) that MSRs can use to confirm the member's identity prior to assisting the member. This function key accesses the *Verify Member* screen which contains information such as the member's code word and birth date.

"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.

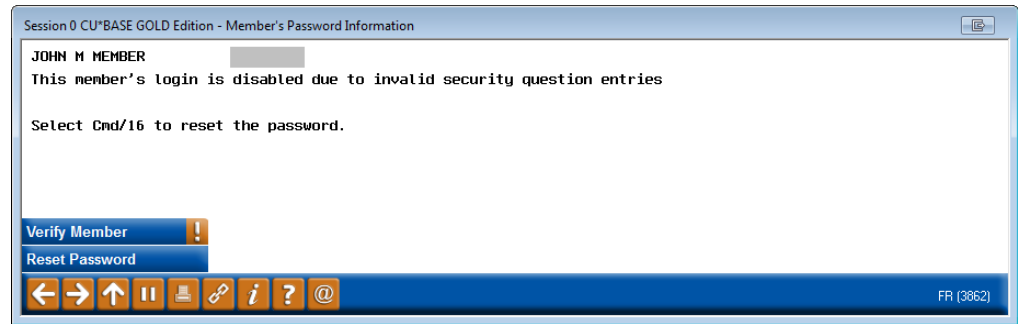
RESET FOR THREE INCORRECT SECURITY QUESTION ANSWERS

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.

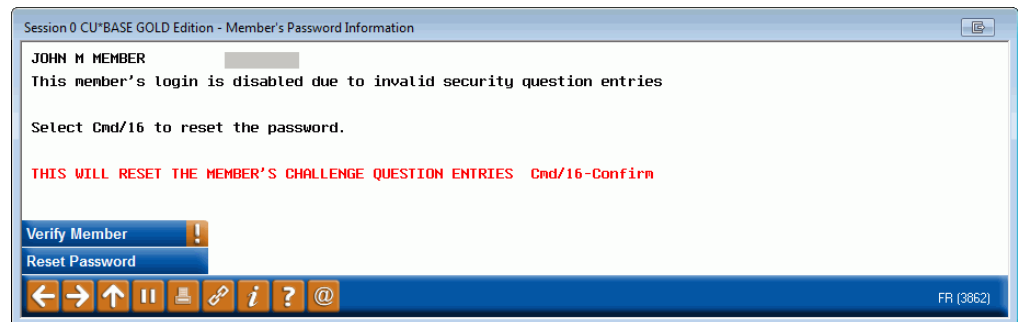
This process clears the answers of the security questions and also resets the member’s password to the temporary password. Once reset, the member will have 24 hours to log in using the temporary password (according to temporary password rules). Once logged in the member will be required to

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

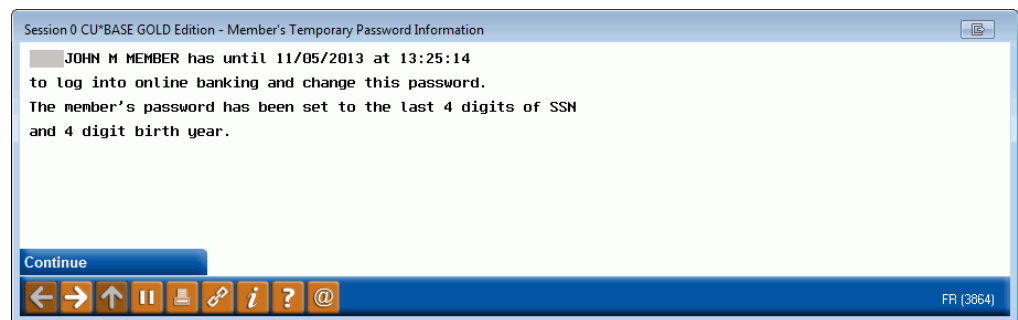


“Reset” (F16) Selected



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

Reset Button Selected



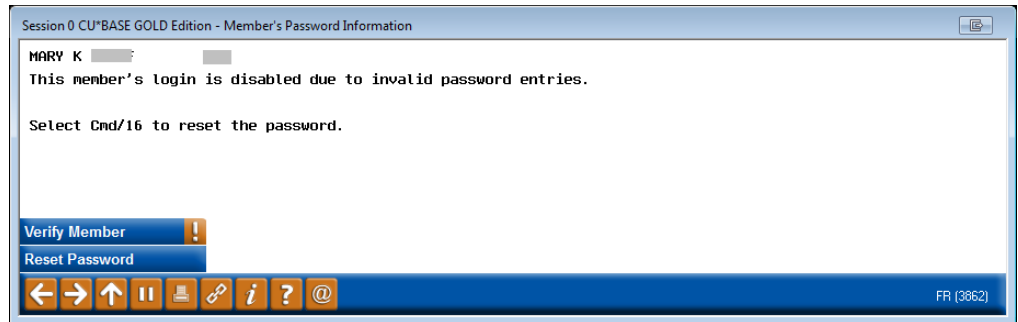
This screen clearly explains that the password has also been reset to the temporary password.

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 24).

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

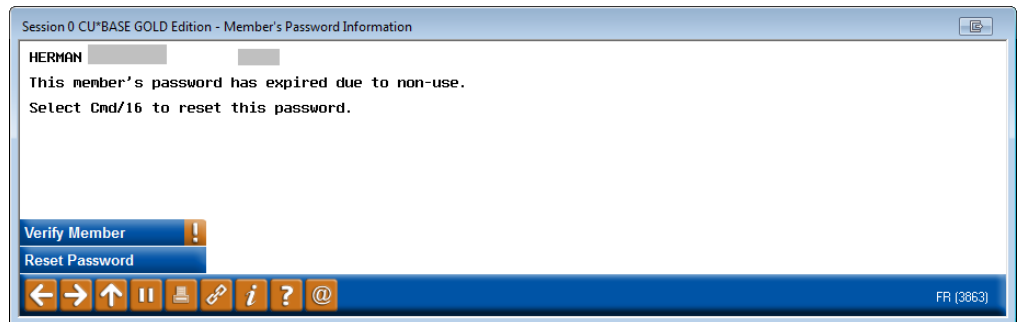


The other screens the MSR will see when assisting this member are similar to the ones the MSR sees when assisting a member who has entered their password incorrectly.

RESET PASSWORD EXPIRED DUE TO NON-USE

In the credit union ARU/Online Banking Configuration, 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 ARU/Online Banking configuration to require usernames. In this case, all members must create a username. **See Page 28 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 29.

Usernames can be a maximum of twenty characters.

OPTIONAL USERNAME

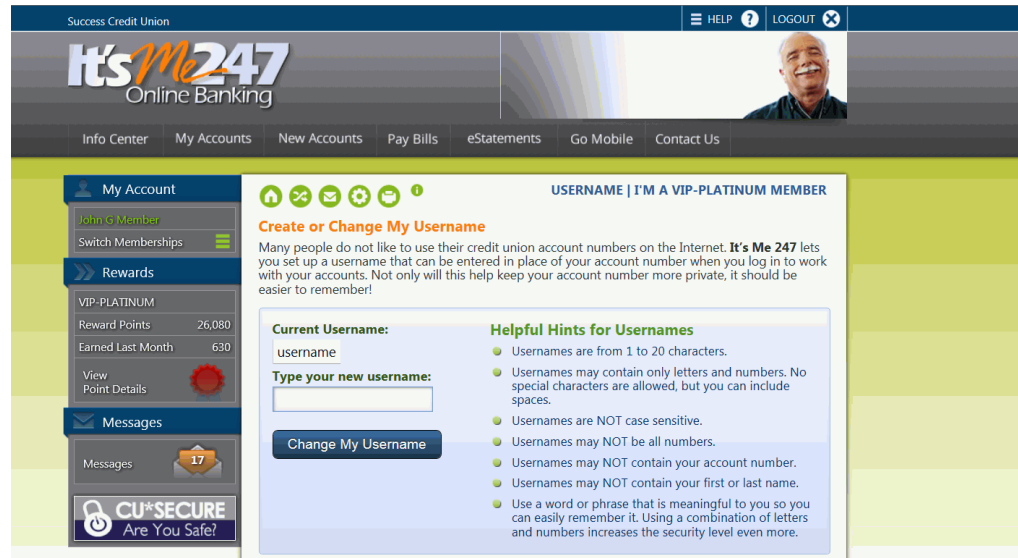
If your credit union does not require usernames, a member can create an *optional username* while in **It's Me 247**. The member can access the Username page via Info Center, then My Username. The member enters the username and then clicks the *Change My Username* button.

Member Creates Username Online (Not required)

The screenshot shows the 'It's Me 247' online banking interface. At the top, there's a navigation bar with 'HELP' and 'LOGOUT' options. Below that, the 'It's Me 247 Online Banking' logo is displayed. A navigation menu includes 'Info Center', 'My Accounts', 'New Accounts', 'Pay Bills', 'eStatements', 'Go Mobile', and 'Contact Us'. The main content area is titled 'USERNAME | I'M A VIP-PLATINUM MEMBER' and features a 'Create or Change My Username' section. This section includes a text input field for the 'Current Username', a 'Type your new username:' input field, and a 'Change My Username' button. To the right of the input fields, there are 'Helpful Hints for Usernames' listed as bullet points. The sidebar on the left shows 'My Account' for 'John G Member', 'Switch Memberships', 'Rewards' (VIP-PLATINUM, 26,080 Reward Points, 630 Earned Last Month), 'Messages' (17), and a 'CU*SECURE Are You Safe?' security notice.

Then at any time, the member can return to this screen to change their username.

Member Updates Username



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. 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

Success Credit Union

HELP ? LOGOUT X

It's Me 247
Online Banking

Info Center My Accounts New Accounts Pay Bills eStatements Go Mobile Contact Us

My Account
John G. Member
Switch Memberships

Rewards
VIP-PLATINUM
Reward Points 26,080
Earned Last Month 630
View Point Details

Messages
Messages 16

CU*SECURE
Are You Safe?

USERNAME | I'M A VIP-PLATINUM MEMBER

Create or Change My Username

! You do not yet have a username. You must set one up before proceeding to your accounts.

It's Me 247 requires that you set up a username to use instead of your account number when you log in to work with your accounts. This helps keep your account number more private. Use a combination of letters and numbers (and spaces, if you want) to create a name that's easy for you to remember.

Current Username:

Type your new username:

Change My Username

Helpful Hints for Usernames

- Usernames are from 1 to 20 characters.
- Usernames may contain only letters and numbers. No special characters are allowed, but you can include spaces.
- Usernames are NOT case sensitive.
- Usernames may NOT be all numbers.
- Usernames may NOT contain your account number.
- Usernames may NOT contain your first or last name.
- Use a word or phrase that is meaningful to you so you can easily remember it. Using a combination of letters and numbers increases the security level even more.

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.

Update Audio/Online Banking Access Screen

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

- Online banking Reason: D02
- 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

Verify Member Skip Password History PIB Reset Security Quest Theme

Start Page Photo Album Display Username

FR (3723) 11/04/13

After confirming the member's access using *Verify Member* (F1), the MSR can either view or delete the member's username by selecting *Display Username* (F20).

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.

Employee Views and Deletes Username in CU*BASE

Session 0 CU*BASE GOLD Edition - Inquire/Delete Members Online Banking Username

JOHN M MEMBER

Member's online banking username is: USERNAME

Be sure to confirm the caller's identity before disclosing or deleting the username.

Verify Member

Delete

FR (3861)

ESTATEMENT 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.

UN-ENROLLING A BATCH OF MEMBERS

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 “ on the Auditing Menu (MNAUDT) menu

The screenshot shows a software window titled "Session 0 CU*BASE GOLD Edition - Batch Un-enroll Members from E-Statements". The window contains the following elements:

- Corp ID:** 01
- Report Options:**
 - Processing type:** Radio buttons for **Audit** (selected) and **Update**.
 - Print report**
 - Export to file**
- Job queue:** A separate box with **Job queue**, **Copies** set to 1, and **Printer** set to P1.
- 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 bar:** Includes back, forward, up, down, print, refresh, help, and search icons.
- Footer:** FR (4339)

OPTIONAL FEATURES MEMBERS USE TO SECURE ACCESS

HIDE MY TYPING



It's Me 247 has tools in place to assist members with securing their access to their online banking account.

When logging into **It's Me 247** members have the option of selecting a "Hide my Typing" feature so that when they enter their security question answer, asterisks appear on the screen in place of the actual characters that they type. This assists members who may not be logging into online banking in a private area.

PASSWORD STRENGTH EDUCATION TOOL

When a member creates or changes his or her password on the My Password page under Preferences in **It's Me 247**, the "Password Strength Meter" tool educates the member as to the security level associated with the password they have just entered. Color coding and messaging help the member determine if the password is "too short" or "weak" (red), "good" (yellow), or "strong" (green).



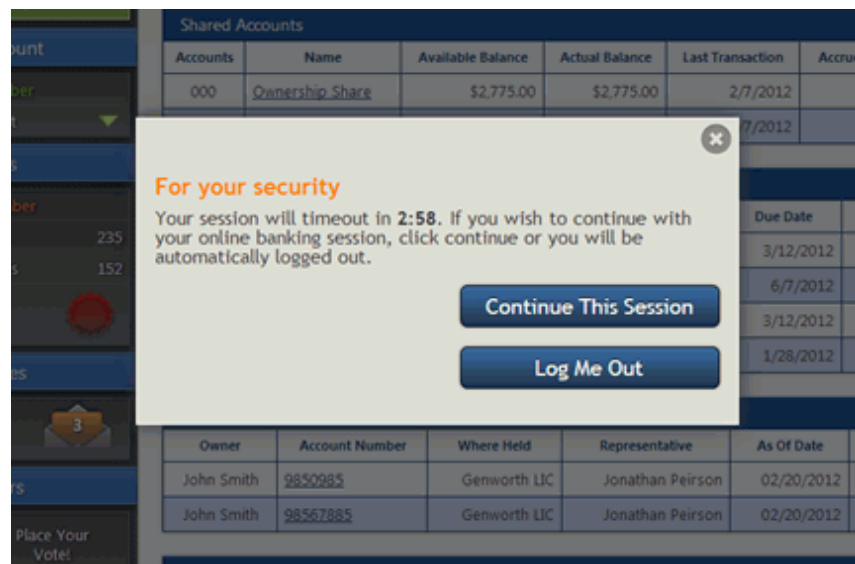
TIMEOUT NOTIFICATION

As a security feature, members are automatically logged out of **It's Me 247** and mobile web banking 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 minute of inactivity.)

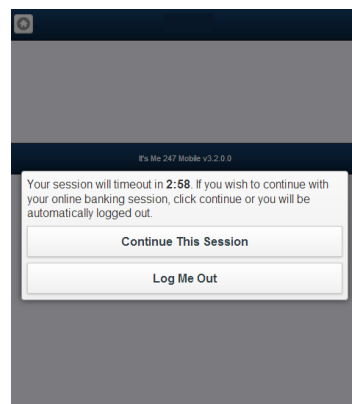
Members are alerted after twelve minutes of inactivity with a pop-up window that counts down the remaining three minutes. If the member clicks "Continue This Session," the timer will be reset and the page will not be refreshed (so the member will not lose anything they have done on the page). If the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

- Members who use either this logout button or the Logout button at the top of the page will be directed to the Online Banking Community (OBC) page. Your credit union can select a different landing page, however. Contact the Internet Retailer Support Center to activate this feature at irsc@cuanswers.com.

"It's Me 247" Timeout Notification

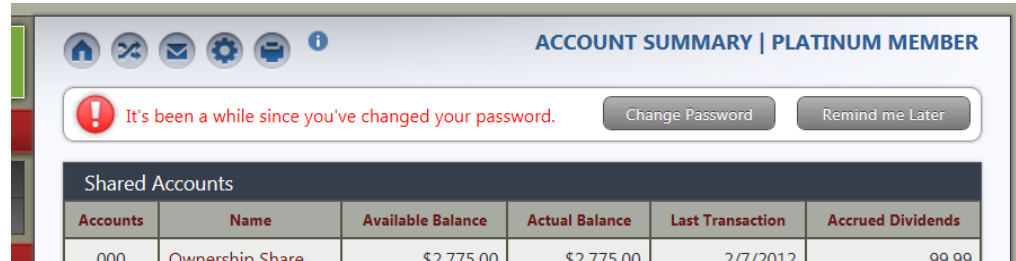


Mobile Web Banking Timeout Notification



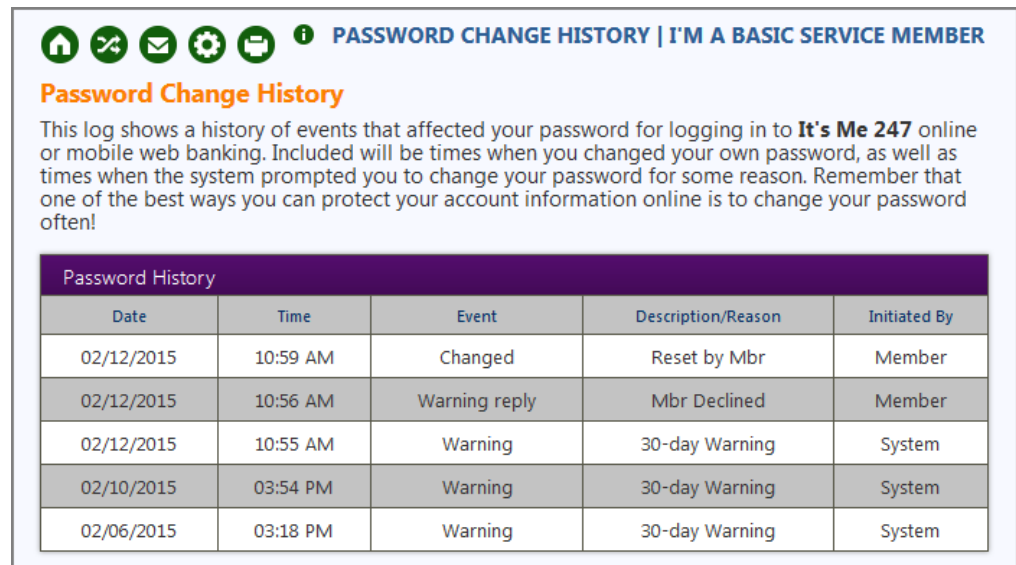
PASSWORD CHANGE REMINDERS

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 Password* 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 “Info Center” section in online banking.



Members changes are recorded in CU*BASE on the PIN/Password change dashboard. **See Page 41.**

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 **Work Online Banking Apps/Req** on the Member Service (MNSERV) menu. 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.

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

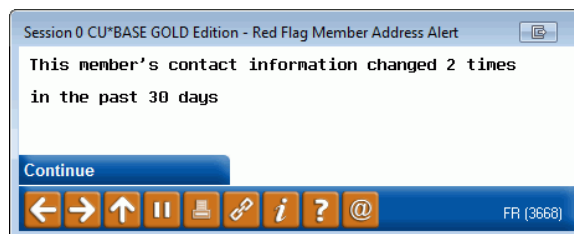
If the member makes any changes to the other information included on the *Personal Information* page in **It's Me 247**, the system generates an online banking confirmation message. These messages are sent both if the change is made by the member online or by an employee in CU*BASE.

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 **Red Flag Controls** on the General Configuration 1 (MNCNFC) menu.

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)

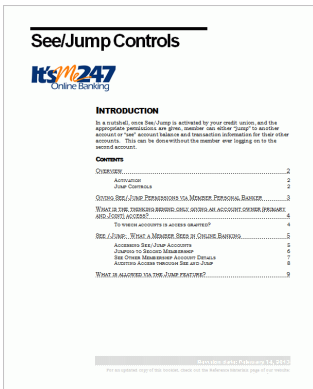
This configuration allows the credit union to select which CU*BASE options will display the message in CU*BASE, including:

- Teller
- Inquiry
- Phone Operator
- Payroll - **Payroll Member Inquiry** on the ACH/Payroll (MNACHP) menu
- ATM/Debit card maintenance – **ATM/Debit Card Maintenance** on the Online ATM/Debit/Credit Card Processing (MNATMD) menu
- Updating/ordering credit cards – **Update/Order Online Credit Cards** on the Online ATM/Debit/Credit Card Processing (MNATMD) menu
- Member Personal Banker (**Member Personal Banker** on the Member Service (MNSERV) menu)
- ATM/DR card account activity (**ATM/Debit Card Activity** on the Online ATM/Debit/Credit Card Processing (MNATMD) menu)

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?

SEE/JUMP ACCESS CONTROLS

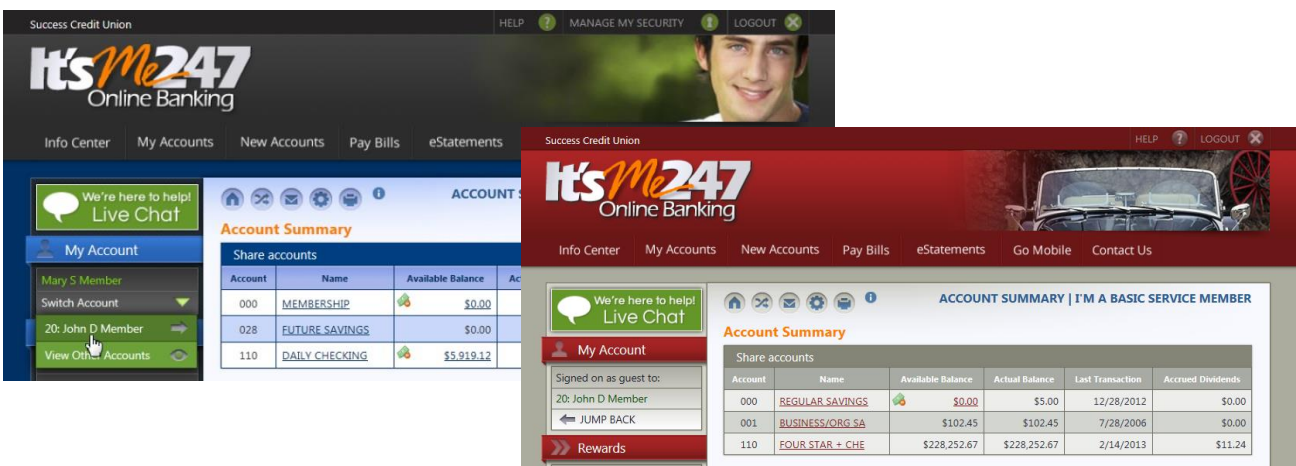


To learn more about this feature, be sure to check out the See/Jump Controls booklet, located on the **It's Me 247**:

http://www.cuanswers.com/pdf/cb_ref/see_jump.pdf

In a nutshell, once this feature is activated and the appropriate permissions are given, the member can either “jump” to another account or “see” account balance and transaction information for their other accounts.

- Your biggest user of See and Jump will probably be a member with multiple memberships at your credit union. Although we package See and Jump together, you may wish to market them separately to your membership.



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.

See is perfect for members who want to be able to monitor balances and transaction activity for another account, but don't need full access to perform transfers or conduct other transactions. The member remains in their original account but can also view the Account Summary and Detail screens for their other accounts. Like Jump, permission can be granted to accounts with the same Social Security Number or to any joint owner on the base (000) account who also has a credit union membership.

For a more in depth look at this discussion, which forms the basis for the decision to only give access to owners via See and Jump, refer to the following 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 #10 Credit Union Configurations, then #8 ARU/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 MNUPDT **Update ARU/Online Bank Transfers** on the Update Functions 1 (MNUPDT) menu or via **ARU/Online Bank Transfer Control** on the General Configuration 2 (MNCNFC) menu. 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, John Member is on this member's Transfer Control list.

The screenshot shows a mobile banking interface. On the left is a navigation menu with options: My Account (Mary S Member, Switch Account), Rewards (VIP-PLATINUM, Earned Last Month: 500, View Point Details), Messages (108), and Members. The main content area is titled "Movin' My Money Around" and includes a brief explanation of the transfer process. It features three steps: "Step 1. When do I want it to happen?", "Step 2. Where am I getting the money?", and "Step 3. Where's it going?". Under Step 3, there are sections for "My CU accounts" (listing 000 - Membership: \$0.00, 110 - Daily Checking: \$7,787.46, 866 - Visa - Daily: \$80.13, and 920 - Mg - Odd Items: \$0.00) and "Other member accounts" (listing John D Member (20) accounts: 000 - Regular Savings, 001 - Business/Org Sa, 110 - Four Star + Che, and 920 - Mastercard Gold). A "What I have so far:" summary box on the right shows: When? Right Away; From Where? 110 - Daily Checking: \$7,787.46; To Where?; How Much?; and Memo:.

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 **Mr PIN/Password Change History** on the Miscellaneous Processing (MNMISC) menu. 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 34** for details and what the member sees in online banking.

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

“Mr PIN/Password Change History” on the Miscellaneous Processing (MNMISC) menu

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	IUR	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	IUR	UPIN	+4
	Apr 13, 2015	09:40:17	Disabled	Disabled by CU	WWW	UPIN	+4

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 of time 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 expiration days in your ARU/Online Banking configuration in OPER).

To keep an eye on members who are activated but have not logged into **It's Me 247** in a while use **Audit Disabled/Inactive PIN/PW** on the Auditing (MNAUDT) menu. 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/PW" on the Auditing (MNAUDT) menu.

Report Sample

ACCOUNT	BASE	MEMBER NAME	PHONE NUMBERS	LAST LOG-IN DATE	LAST CHANGED DATE	DAYS SINCE LAST LOG-IN	STALE PASSWORD	DISABLED PASSWORD	CHALLENGE QUSTN/ANS
7916		SHANNON L MEMBER	Home: 555-555-5555 Work: 222-2222	11/02/2009	11/05/2009	77		Y	Y
38810		CARISSA J MEMBER	Home: 777-777-7777 Work: 777-888-8888	11/04/2009	11/20/2009	75		Y	Y

Additionally if you wish, you may use the CU*BASE Report Builder to Query the **PCMBRCFG** file, and looking at the Last Logged In Dates and comparing them to a certain point in time, you should also be able to find members that:

- Are activated and use **It's Me 247** regularly
- Are activated but have never signed on to **It's Me 247**
- Have been deactivated

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.

Effective Date: November 16, 2015

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 in order to permit access through the SYSTEM. The first time you login to Online Banking, 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. The 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 the 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 the credit union.

7. The technical requirements to assure that you have the ability to access and retain your eStatements and other electronic disclosures are described in this section. 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 which 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 E-Statements and other electronic documents, you must have access to a printer or the ability to download information in order to keep copies of electronic documents for your records.

8. You understand and agree that you must notify the 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 the 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. 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 E-Statements 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

BILL PAY TERMS AND CONDITIONS

Service Definitions

"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.

"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.

"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.

"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.

"Scheduled Payment Date" is the day you want your Biller to receive your bill payment and the next day will be the day your Payment Account will be debited, unless the Scheduled Payment Date falls on a non-Business Day, in which case it will be considered to be the previous Business Day.

"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.

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

HARDWARE AND SOFTWARE REQUIREMENTS

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 Adobe Reader. You are solely responsible to obtain such hardware and software.

CHANGES TO HARDWARE OR SOFTWARE REQUIREMENTS

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.

TRANSFER LIMITATIONS

There is no limit on the number of transfers from your savings account or your MMSA 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 MMSA to six per calendar month. The types of transfers that are limited are those requested by fax, telephone, internet, and pre-authorized transfers.

ENHANCEMENTS/MODIFICATIONS TO SERVICE

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

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. In order 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 the credit union in the filing of a petition of bankruptcy, the 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

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 all of your savings and checking transaction activity through Account Access.

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.

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 CLOC 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.

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.
- In order to verify the existence or conditions of your account for a third party, such as a credit bureau or merchant.
- In order 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

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 us 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.

IMPORTANT INFORMATION ABOUT BECOMING AN AUTHORIZED USER

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

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.

CHARGES OR FEES

Charges for the Bill Pay service, other transactions and optional services (e.g., non-sufficient funds or stop payment fees) are specified in CREDIT UNION's *Schedule of Fees & Charges*, which can be found on the CREDIT UNION website.

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

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:

1. You will reimburse the Service immediately upon demand the transaction amount that has been returned to the Service;
2. 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;
3. You will reimburse the Service for any fees imposed by your financial institution as a result of the return;
4. You will reimburse the Service for any fees it incurs in attempting to collect the amount of the return from you; and
5. 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' *Schedule of Fees & Charges*, which can be found on the CREDIT UNION

website (www.cuanswers.com). 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.

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

The earliest possible Scheduled Payment Date 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 scheduled Payment Date less than the earliest possible Scheduled Payment Date designated for each Biller. When scheduling payments, select a Scheduled Payment Date that allows adequate time for delivery prior to any late date or grace period.

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:

1. 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;
2. 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.
3. You have not provide the Service with the correct Payment Account Information, or the correct name, address, phone number, or account information for the Biller; and/or
4. 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.

PAYMENT METHODS

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.

STOP PAYMENT REQUESTS

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' *Schedule of Fees & Charges*, which can be found on the CREDIT UNION website (cuanswers.com).

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.

PASSWORD AND SECURITY

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.

YOUR LIABILITY FOR UNAUTHORIZED TRANSFERS

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

In case of errors or questions about your transactions, you should notify us as soon as possible.

If you think your statement is incorrect or you need more information about a Service transaction listed on the statement, we 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 us 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 us the dollar amount of the suspected error.

If you tell us verbally, we may require that you send your complaint in writing within ten (10) Business Days after your verbal notification. We 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 we require more time to confirm the nature of your complaint or question, we reserve the right to take up to forty-five (45) days to complete our investigation. If we decide to do this, we will provisionally credit your Payment Account within ten (10) Business Days for the amount you think is in error. If we ask you to submit your complaint or question in writing and we do not receive it within ten (10) Business Days, we may not provisionally credit your Payment Account. If it is determined there was no error, we 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 our investigation. The Service may revoke any provisional credit provided to you if we find an error did not occur.

DISCLOSURE OF ACCOUNT INFORMATION TO THIRD PARTIES

It is our general policy to treat your account information as confidential. However, we 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' privacy policy.

ALTERATIONS AND AMENDMENTS

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.

ADDRESS OR BANKING CHANGES

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 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.

SERVICE TERMINATION OR SUSPENSION

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

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 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

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.

ASSIGNMENT

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.

NO WAIVER

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.

CAPTIONS

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.

GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws of the State of Michigan, 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.

ELECTRONIC DISCLOSURES

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

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 your the CREDIT UNION' address of record. In addition, the CREDIT UNION' will provide changes to the terms of this Electronic Disclosures Agreement and other related disclosures electronically.

HARDWARE AND SOFTWARE REQUIREMENTS

To access and retain copies of your online statements and to utilize the Payveris Bill Pay Service and to receive other related notices, you must have Internet access with a compatible browser. You may also need Adobe Reader. You are solely responsible to obtain such hardware and software.

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 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.

COMPLETE AGREEMENT, SEVERABILITY, CAPTIONS AND SURVIVAL

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