JUNE 2018
Version 1.0

SecuriKey

CU*ANSWERS

Risk Assessment for It's Me 247

Online Banking

It's Me 247 Online Banking

CU*ANSWERS
A Credit Union Service Organization

CONTENTS

LEGAL DISCLAIMER

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

INTRODUCTION

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

While this document is intended to assist credit unions in their risk assessments, note that not all features and tools listed are automatic. Many security tools must be specifically activated by the credit union. For example, many of the security features are available in Personal Internet Branch (PIB).

Both **It's Me 247** Online Banking and Mobile Banking use the same authentication features. PIB is available for Online Banking, and Multiple Authentication Choice Options ("MACO") is available for Mobile Banking. See the *SecuriKey MACO* document for more information.

FEATURES

256-character password availability

256-bit encryption for authentication information transmitted

Optional Personal Internet Branch (PIB) for layered security

LEARN MORE

You can download the PIB manual here.

QUICK REFERENCE

LOGIN

256 Character Password Limit: Minimum limit is 6-20 characters.

Challenge Question: Members must answer a challenge question at login.

Incorrect Login: Account is disabled if three incorrect passwords are entered, or three incorrect challenge questions.

Temporary Password: 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**.

Password Expiration: Online banking passwords can be configured to expire after a certain period of non-use.

Timeout: Members are automatically logged out of **It's Me 247** after fifteen minutes of inactivity or page refresh (five for login and security screens).

Red Flag Warnings: 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 the personal information items in the last 30 days.

DATA TRANSMISSION

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

Data Storage: Username and password information is "salted" (random data added) and hashed.

PIB LAYERED CONTROLS (OPTIONAL)

Geographic Controls: Allows or blocks access based on the PIB profile.

PC Registration Controls: Members can require that a computer be registered before it can be used to sign on to **It's Me 247**.

Days and Times Available: Members can use these to establish what is "normal" for them, blocking access during days and times when they will never be using **It's Me 247**.

Confirmation Codes: Members can set a confirmation code (essentially an additional password) for EFT transactions and transfers, as well as loan applications. Bill Pay and new accounts can be configured to require confirmation codes.

Secure Message Center: If changes have been made to a member's PIB Profile, or if someone has attempted to access the member's **It's Me 247** accounts in violation of a PIB profile setting, a message is sent to the member's **It's Me 247** secure Message Center.

RISK ASSESSMENT TOOLS

Username and Password Features

It's Me 247 Online and Mobile Banking offers many controls for managing the passwords used by members to gain access to their accounts.

Usernames. Usernames can contain a letter or a combination of letters and numbers. They are not case sensitive and can include spaces and cannot contain special characters. Usernames that contain the account number and or member's first or last name will not be accepted. Future releases may allow this to be credit union configurable.

Password Disabled. Three incorrect attempts disable the password**.**

Password Length. Online banking passwords can be up to 256 alphanumeric characters, including special characters

Password Characteristics. Passwords are case-sensitive (i.e., Ds443&sld is different from dS443&SLD). Passwords can include a blank space. **Passwords are not stored on the It's Me 247 server system**.

Password Minimums and Maximums. Credit unions can specify a minimum number of characters. The minimum can must be at least 6 characters, with maximum as many as 256 characters.

Complex Passwords. Credit unions can require members to follow complex password rules (requires three of the four following: uppercase letter, lowercase letter, number, and special character).

Hide Typing. When logging into **It's Me 247** members have the option of selecting a "Hide my Typing" feature (by clicking the eyeball graphic) so that when they enter their security question answer, asterisks appear on the screen in place of the actual characters that they type.

Password Strength Meter. 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. A password strength indicator is presented to dynamically measure the strength of their password as the member enters it.

Account Non-Use. For credit unions who set this feature, members will receive a warning if their online account will expire for non-use.

Password Change Warning Message. The password change warning message will remind members they should consider changing their password, and track when the member clicks "Remind Me Later."

Challenge Questions

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. The challenge question rotates, the member selects from a list and creates one.

Three incorrect challenge question answers require the credit union to reset the account.

Temporary Password

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. Temporary passwords expire after 24 hours.

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. A temporary password reset by the credit union is valid for 24 hours.

- Once members log in to **It's Me 247** the member be required to immediately change their online banking password.

- New memberships can set how long a period (from one to seven days) that the new member temporary password is valid.

- Online banking passwords can be configured to expire after a certain period of non-use, either a configured number of days (1-90) or select 999 days to never expire passwords due to non-use.

Session 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. The login and security screens the only exceptions. Members are logged out of these screens m after five minutes of inactivity.

Members are alerted after twelve minutes of inactivity with a pop-up window that counts down the remaining three minutes. If the member clicks “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.

Red Flag Warnings

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 the personal information items in the last 30 days.

Authentication Information

Authentication information entered by the member is encrypted. Transmission security is provided by using 256-bit encryption. Passwords are then “salted” for additional security, hashed, and the 256-bit string is compared to the value stored in the database.

PIB TOOLS

The Personal Internet Branch (PIB) System provides layered security controls and member personalization for the **It’s Me 247** Online Banking application. The configuration of PIB settings involves two parts: the PIB default profile configuration itself, and the master ARU/Online banking configuration settings that control the availability of certain features for the credit union. PIB default profile configuration allows individual members to make decisions about their security, rather than having security unwillingly forced on every member.

Geographic Controls. **It’s Me 247** uses geo-location technology to determine the approximate geographical location of the computer being used to authenticate into online banking. Members can use this to only allow online banking access within a configured geographical location.

PC Registration Controls. Members can require that a computer be registered before it can be used to sign on to **It’s Me 247**. This is done using a special type of cookie called a "persistent" cookie that contains encrypted data that is stored on the user’s hard drive for use by the browser software. When a member attempts to log in to **It’s Me 247**, the system looks for that cookie on that computer and will not allow the member to log in if it is gone.

Days and Times Available. Members can use these to establish what is “normal” for them, blocking access during days and times when they will never be using It’s Me 247. This provides another layer of security by narrowing the window of times when their accounts could potentially be accessed by an unauthorized person.

Confirmation Codes. Members can set a confirmation code (essentially an additional password for EFT transactions and transfers, as well as loan applications.

Secure Message Center. If changes have been made to a member’s PIB Profile, or if someone has attempted to access the member’s **It’s Me 247** accounts in violation of a PIB profile setting, a message is sent to the member’s **It’s Me 247** secure Message Center.

ABNORMAL ACTIVITY

Credit unions can monitor high risk online banking activity through the Abnormal Account Activity Monitoring function. This allows a credit union to define the ranges (number of transactions and dollar amount) of a month's worth of transaction activity that you would consider normal, abnormal, and high risk for the group.

Online banking activity that can be monitored (among other transactions) include:

> **Share Draft from Bank Process**. This includes all checks posted to member accounts via daily share draft processing, including member checks processed via **It's Me 247** Bill Pay.
>
> **ACH Network Processing**. ACH activity, including debits for online bill payments that are processed via **It's Me 247** Bill Pay.

FEATURE MATRIX

(A) Types of information that can be seen about the member should an unauthorized person gain access to a member account via It's Me 247.

(B) Actions that can be taken with the member's information or money should an unauthorized person gain access to a member account via It's Me 247.

(C) Marked if the feature is considered a special security feature of the online banking software to help prevent unauthorized access or alert members of unauthorized activity.

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
Security Features				
Password security	• The credit union can select minimum number of characters. This minimum must be 6 characters, maximum 256. • The credit union can optionally select to force complex password rules. This requires three of the four of the following: uppercase letter, lowercase letter, number, and special character. • Regardless if complex passwords are required, members can use numeric, alphabetic, and special characters in the passwords. Passwords are case-sensitive.	--	--	Yes
Temporary password	• This system-generated password used for new members, members whose password is reset by a credit union employee, or the password used during a promotional campaign for **It's Me 247**. • The credit union selects one of the four temporary password settings. They include: birth year and first two letters of last name (all capital letters), last 4 of SSN and birth year, last four of SSN, or first 4 of SSN and first two letters of first name (all capital letters). • Temporary passwords are only available for 24 hours. If the member does not log into online banking and change the	-- password not visible to member or CU staff; encrypted in CU*BASE files	Password can be changed	Yes

CU*ANSWERS
A Credit Union Service Organization

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	password in 24 hours, the password expires, and the member must have the password reset again. • The member is required to change the temporary password immediately after logging into online banking for the first time. The member is not allowed to set a new password that matches the temporary password.			
Security questions and answers	• Members must answer a security question and a password each time they log into online banking. • Members set up three questions and answers the first time they log into online banking. The member is given the option of composing both the question and answer for one security question. • Security questions can also be set up in Mobile Web Banking (for example on the member's phone during the membership opening process). • Security question answers can be a maximum of 30 characters, allowing members to create a phrase as an answer. • Security questions are also used when members reset their passwords through the "I forgot my password" feature. Members must answer all three security questions correctly to reset their password. • Member Service representatives can delete security questions and answers (first following credit union policies). In this case, the member will set up security questions next time the member logs into online banking.	-- security question answer available in Query; member can elect to hide answers when typing it in a public area (see below)	Security questions and answers can be changed	Yes
Restricted password/ security question retries	• Members are only allowed 3 attempts to enter the correct password and security question answer combination before the password is disabled. • This feature is used to prevent someone from trying to "guess" a member's password or security question.	--	--	Yes
Reset of disabled password	• Once password is disabled, a credit union employee can reset the disabled password to the default password setting (see previous section on credit union options). Member is required to change password upon first access.	--	--	Yes

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	• Member can also use the "I forgot my password" feature to reset their password. The member must answer all three security questions correctly to reset their password.			
Member notification of password change	• Members receive an email notification and a message in their Secure Message Center in online banking every time their password is reset, regardless of who resets the password. (A password might be reset by a credit union employee in CU*BASE or by the member in online banking.) • Members can see these password changes in online banking to self-monitor activity on their account – only for their account.	--	--	Yes
Credit union monitoring of password changes	• The Member Password Change History report and online management dashboard lists all online banking password changes. The system tracks use of "Remind Me Later." • Both indicate the reason for the change. Two examples are that a credit union employee reset the password in CU*BASE or member locked the account with three incorrect entry combinations and used the "I forgot my password" feature to rest the password.	--	--	Yes
Username	• Usernames are use in place of account number when member logs into **It's Me 247**. • Usernames are defined by members in **It's Me 247**. Usernames can also be set up in Mobile Web Banking (for example on the member's phone during the membership opening process). • A credit union employee cannot set up a username in CU*BASE for a member. • The first time members log into online banking, their account number is used since a username is not yet defined. • Usernames may not include the member's account number. They may be 1-20 characters, cannot be all numbers, cannot contain the member's first or last name, and are not case sensitive.	username can be displayed to CU staff in CU*BASE	Username can be changed	Yes

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	• Credit union employee can view username of member and assist member who forgets (after first confirming identity of member). • Credit union employees can delete usernames (after confirming identity of member). In this case the member will use the account number until another username is configured by member.			
Required usernames	• Credit union can elect to require usernames. In this case all members are required create a username and use it in place of their account numbers when they login to online banking. (See above for more information on usernames.)	--	--	Yes
New members access	• The credit union can elect to activate **It's Me 247** automatically for new members. They can also require member to request access before manually activating. • The credit union can define the number of days a new member can access online banking with the system generated temporary password before the password expires. Expiration length for new member password can be set to a configured 1-7 days. • The temporary password follows the rules defined by the default temporary password. (See previous section.) • The member is required to change the password immediately on the first access to online banking as with access with any temporary password. (They are not allowed to set a new password that matches temporary password setting) • Members can use Mobile Web Banking to reset passwords (for example during membership opening). Passwords can also be reset in online banking.	n/a	Password can be changed	Yes
"Non-use" password expiration	• Passwords can be configured to "expire" automatically after a certain number of days of non-use • Credit unions can select the number of days (1 – 90 days) • Credit unions can select to never expire a password due to non-use by entering 999 days.	--	--	Yes

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	• NOTE: If a member logs in during this time period, a member's password will not expire • Member may contact CU to have password reset when the password "expires." Or members can use the "I forgot my password" link and answer three security questions to reset the password themselves.			
Deactivate access at member's request	• The credit union can deactivate a member's password altogether so that no access is allowed to online banking.	--	--	Yes
Hide my Typing	• Members can select to use the "Hide my Typing" feature to type the answers to their security answers as asterisks (instead of the actual text of the answer)	--	Extra security feature	Yes
Password Strength Meter	• When members create their passwords, the password strength meter indicates with a colored indicator whether the password is weak or short (red), good (yellow) or strong (green) • This encourages members to select strong (green) passwords	--	--	Yes
Reminder when member has not changed their password in last 30 days	• **It's Me 247** displays an automated "soft" warning message to encourage members to change their password, without making it mandatory. This message will appear when the member has not changed their password for the last thirty days. • Members can elect to change their password or ask to be reminded again in 30 days. • Member's selection is recorded in CU*BASE for auditing purposes. Members can also see their selections online.	--	--	Yes
Evaluation of activated but inactive members	• Auditing report helps evaluate risk of inactive members. • Available on the auditing menu for restricted access. • Lists member who are activated, but have not logged in (for a selected date range)	Member accounts	--	Yes
Usage statistics for CU employee on member access	• Displayed via CU*BASE Inquiry, Phone Op, Teller; shows logons used current and previous month and other self-service status (bill pay, eStatements)	--	--	Yes

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	• Management dashboard show stats for online/mobile web banking, mobile text banking, and audio-response banking). Shows logons used current and previous month and other self-service status (bill pay, eStatements)			
Usage statistics to member	• Details times logged into online banking as well as access point (online banking, mobile banking), jump from other accounts or see balances from other accounts	--		Yes
Confirmation email and secure online banking message for personal information changes	• Members receive confirmation emails and secure message center messages whenever a personal item, such as address, email address, or code word is changed (both via **It's Me 247** by the member or via CU*BASE by a CU employee • If the email is changed, the member receives and email to the old and new email address. • No personal information is shared in the email. Members receive notification of what element has changed but not the actual change itself.	Item that changed, not data	--	Yes
Transfer controls	• Must first activate transfers to other credit union accounts. • Transfer Control is used to limit the member accounts to which funds can be transferred. (Requires password access on the "from" account only) • A: Transfer control configuration restricts transfers to select to: accounts. These relationships must be set up by credit union employee. • B: Transfer control configuration allow for optional restriction to require member to enter specific to: account information (acct # with 3 characters of the last name for confirmation) • Either A, B, or A and B can be used by credit union	--	--	Yes
Online Banking Use Agreement (Member Indemnification)	• Members are required to accept the "**It's Me 247** Online Banking Use Agreement" the first time they access **It's Me 247** • Acceptance date is recorded in credit union files	--	--	Yes

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
Timeout Notification / Session "timeout"	• Members are alerted after twelve minutes of inactivity or page refresh 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.	--	--	Yes
Stand-in processing for 24x7 availability	• Stand-in processing makes online banking services available even during nightly and monthly CU*BASE processing	--	--	Yes
Additional confirmation required when member makes Account-to-Account (A2A) transfer	• If A2A is activated, members must select an additional confirmation checkbox before authorizing an A2A transfer. • Members are then provided a page where they can print the transaction for their records.	--	--	Yes
Personal preferences and security controls	• Includes site styles, personal information update, password changes, username changes, eStatement options, statement style options, etc,	See below and above	See below and above	Yes
Wrong email messaging	• If member's email address is flagged as a wrong email address, member will see message encouraging them to change their email address immediately upon logging in and each time thereafter until email address is updated • Member can click to save the address if it is mistakenly marked as invalid	Email address	--	
Loan coupons	• Members can select to print loan coupons directly from online banking, allowing this to be a self-service feature. Members print these coupons directly from the loan detail screen.	• Member name • Mailing address • Account base • Account suffix	Can be used to pay loan	
eAlerts	• CU can elect to allow members to subscribe for eAlerts online through **It's Me 247** (CU*BASE feature also available for staff to maintain for members and view alerts sent) • Member receives the alert via the **It's Me 247** Secure Message Center	If "long" message selection is selected, email reports the following for clarity • Account Name	n/a	

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	• Member can optionally select to also receive email notification alerting them that an alert has been sent (no account details included in the email – short option) or a "long" email containing more detailed information • If Mobile Text Banking is activated at the member's credit union, and the member is enrolled in Text Alerts, members can also select a fourth option, to receive the alert in the form of a text to their mobile phone • eAlerts balance notifications (email and text message) are evaluated on the 30-minute (configurable for self-processors) cycle. Other emails and text messages are sent according to request, for example ACH Transaction alerts are sent when ACH transactions are posted. • e-Alert types: • Account Balance above or below specified amount (based on available balance) • ACH Deposit and/or Withdrawal posted to account • Loan Payment coming due within specified # of days	• Account Nickname • Suffix If balance eAlert selected, balance information will also be emailed. All other shorter selection options show no private data.		
eNotices	• Allow the credit union to send an electronic version of a printed notice to the member • Members can view their eNotices in their Secure Message Center in Online Banking • Content of eNotice is the same as printed notice, except that member's private information is masked in the eNotice for additional security • Members can select to have an additional email notification sent when the eNotice is sent (having the notification sent via text message is also available if the member is enrolled in Mobile Text Banking). NOTE: Only a notification is sent; the notice text is not included in the notification. • Members can quickly access other online banking pages via helpful links directly in their eNotices, for example to access the transfer screen to pay on a delinquent account (from a delinquency e-Notice) or to change the renewal options (from a CD Maturity e-Notice)		n/a	

Feature	Feature Overview	(A) Member Information That Can Be Seen	(B) Actions That Can Be Taken with Member Money / Info	(C) Considered a Special Security Feature
	• E-Notices email notifications and text messages are sent when notices are printed.			

VERSION CONTROL

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

CU*ANSWERS
A Credit Union Service Organization