It's Me 247 Online Banking

Understanding It's Me 247 Security

A Guide for our Credit Union Clients and Owners

October 2, 2014

It's Me 247 Security Review

CU*Answers is committed to the protection of you and your members.

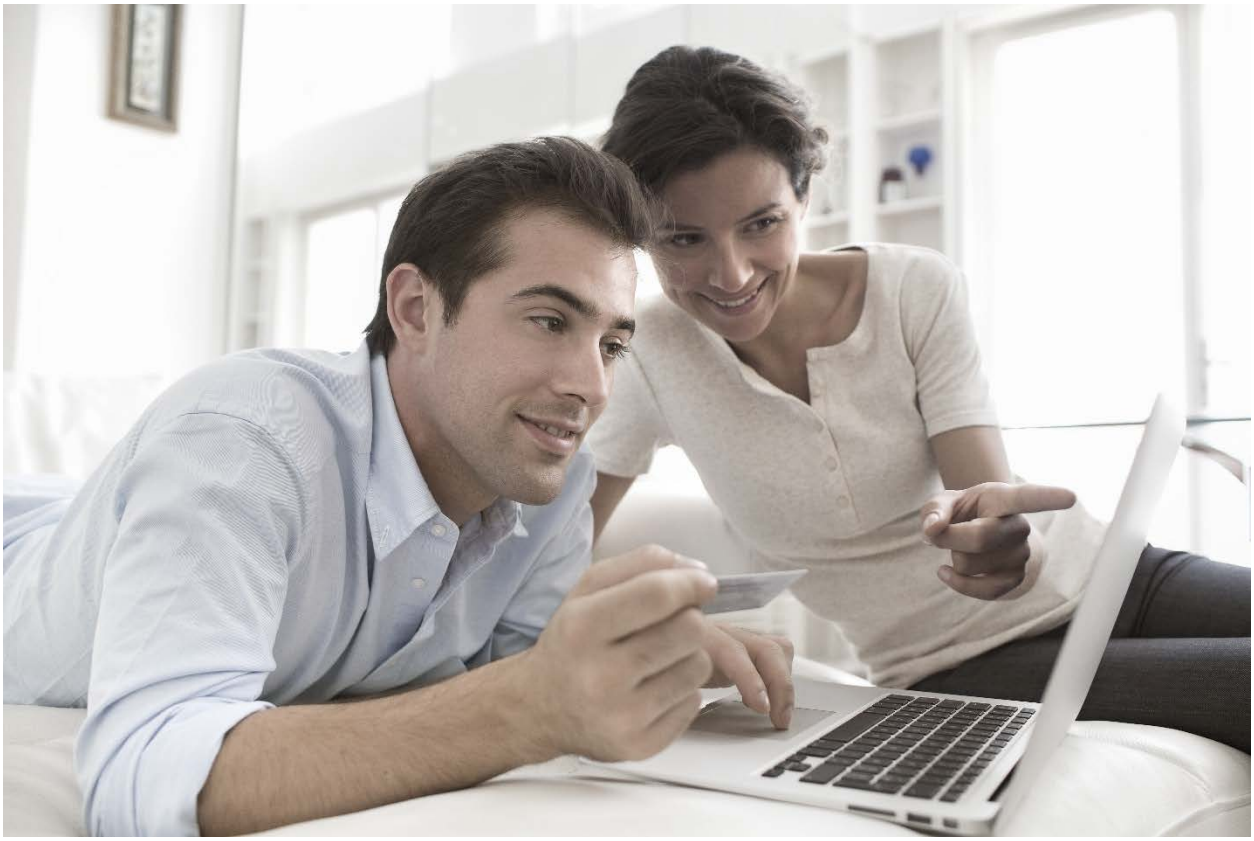
CU*Answers is a cooperative owned and managed by over one hundred credit unions located throughout the United States. Our leadership and staff is dedicated to protecting you and your members from fraud and other risks associated with online banking. While there is no such thing as perfect security, we have a compliance and risk management team that works closely with our programming department to ensure that **It's Me 247** is secure and compliant.

During the 2014 examination cycle, many of our owners and clients have been flooded with requests for information on the security surrounding **It's Me 247**. This handout is intended to help support your team in understanding how **It's Me 247** can protect your members from fraud and identity theft, as well as answer the toughest questions from your examiners. Your feedback is important to us, and helps us develop better products that serve your needs and the needs of your membership.♦

DID YOU KNOW?

CU*Answers has over half a million members (and growing!) logging on to **It's Me 247** each year.

CU*Answers delivers approximately four million Online Banking pages each month.



Key Elements of our Security Program

CU*Answers employs numerous controls to protect against security breaches.

To protect our cooperative enterprise against data and identity theft, CU*Answers has a comprehensive information security program. For security reasons, we do not release the technical details of our program or audit results, but we can offer the key elements of what we do to protect you and your membership.

Highlights of the program include:

Employee Hiring Process
All CU*Answers employees are screened prior to hire, and all employees must be bondable against dishonesty before beginning work at CU*Answers.

Hosting
It's Me 247 is hosted in a protected DMZ environment complete with intrusion detection and firewalls configured to industry standards.

Environmental Protection
It's Me 247 is hosted in a carefully controlled environment, including moisture and temperature sensors and alarms.

Notification
By law and by contract, CU*Answers is required to notify you in the event there is a material breach affecting you or your members.

Log and Alarm Review
Our IT staff reviews logs on a daily basis, and supports a complex infrastructure monitoring system with automated alarms and notification.

Disaster Recovery
CU*Answers has a comprehensive disaster recovery program involving multiple data centers and featuring High Availability for core data processing.

Internal and External Audits
CU*Answers has an internal audit department that tests access and IT controls related to Online Banking. (This is not a substitute for a credit union's own due diligence). In addition, CU*Answers has external audit firms perform network security tests on an annual basis. Our Board of Directors is always notified of internal and external audit findings.

Examinations
As with your credit union, CU*Answers undergoes regular IT examinations by the NCUA, as well by state supervisory authorities. **By law**, CU*Answers may not release any of these findings but your examiners may contact the State of Michigan for information relating to our examinations. ♦

DID YOU KNOW?

Your credit union can go above and beyond the basic FFIEC and NCUA requirements for online banking by turning on Personal Internet Branch ("PIB").

PIB allows you and your members to decide on how to increase the security of the online banking system.

CU*Answers offers guidance and a step-by-step process for turning on PIB features for your membership:

Set custom/complex PIN and passwords
Email notification for password changes
Transaction dollar limits
Transaction time limits
Confirmation codes

And much more.

CU*Answers also has a step-by-step guide for turning on PIB:

If you haven't already, CU*Answers strongly recommends reviewing what PIB offers to see if these security tools are right for you and your membership.

Answering the IT Questionnaire

CU*Answers can help you and your staff understand and answer the standard IT Online Banking Questionnaire used by the NCUA.

*While CU*Answers cannot answer every one of the 90+ questions your examiners may ask, we can provide guidance to help you answer the questions yourself or direct you to the resources which may help your credit union complete the requirements faster.*

*Some questions that CU*Answers cannot answer (credit union only questions) have been omitted.*

2a and 2b

Is the credit union utilizing an external vendor to provide the electronic banking services?

If yes, has appropriate due diligence been performed on the third party electronic banking provider?

Performing Due Diligence on CU*Answers

*CU*Answers provides guidance on how to conduct due diligence on our cooperative, including Online Banking:*

3

Does management review external audits or reviews relating to their electronic banking service?

SSAE-16

*CU*Answers contracts external firms to conduct penetration tests and network security assessments on an annual basis, and conducts an external SSAE-16 every 18 months. While CU*Answers does not publish the results of the network security assessments and the penetration tests, the SSAE-16 can be downloaded here:*

*CU*Answers management and board of directors receive reports of all findings and remediation actions taken as a result of external audit activities.*

4

Has management performed a risk assessment to address the risk of each electronic banking service provided?

Risk Assessment Template

*CU*Answers conducts its own internal and non-public risk assessments. However, your credit union can complete its own (required) risk assessment using our template:*

Important Note

Always remember that your credit union has the ability to make some security choices based on the needs of your membership. CU*Answers provides a large set of Online Banking security tools to help your institution, but the fact that you decide to not deploy some or all of these options does **not** mean you are out of compliance. Online banking compliance is a fluid concept that changes based on the risk profile of your membership, and evolving technology standards.

Critical Question Review

5

Has management evaluated E-banking solutions for compliance with FFIEC authentication guidance?

FFIEC Whitepaper

Your credit union can review its own compliance with FFIEC requirements by reviewing this whitepaper:

6

Are appropriate controls in place for personnel with electronic banking duties (manage/access the system)?

*CU*Answers employs access controls consistent with industry best practices.*

7

Does management adequately monitor system reports for suspicious or unauthorized access?

*CU*Answers does daily log checking for suspicious or unauthorized access.*

8

Are policies, procedures, and/or practices in place for User IDs and passwords for E-banking systems that address:

8a

Strong password selection?

Available

8b

Do user names and passwords for electronic payment systems avoid use of account numbers or personal identifiers such as social security numbers?

Available

8c

Is there a secure process for opening new E-banking accounts?

Available

8d

Maximum number of bad login attempts before locking out members?

Always

8e

Procedures to reauthorize members who are locked out of their accounts?

Always

8f

Require members to change their password the first time they access the account and after being unlocked/reset?

Available

9

Do electronic banking sessions time out after periods of user inactivity?

Always

10

Does the electronic banking system have reasonable transaction limits consistent with normal usage?

Available

11

Do E-banking solutions have alerting features that notify members when transactions of elevated risk occur?

Available

12

Are inactive accounts disabled or purged after a defined number of days?

Always

*The answers to questions 8-12 may be dependent on the settings the credit union has selected for **Its Me 247**.*

Important Note

CU*Answers, like your credit union, is a cooperative. This means our company is operated by you (and in some cases also owned by you). Your input and the input of your peers is what CU*Answers uses in developing new technology and solutions for your members. If you find that there is a solution your members need in Online Banking or other CU*Answers product, get with your peers and use the Idea Forms to let us know!

FFIEC Authentication Guidance

13

Does the credit union have a documented risk assessment process for all electronic banking services covered by the 2005 FFIEC Authentication Guidance & 2011 Supplement?

Risk Assessment Template

FFIEC Whitepaper

16

Has management developed a written action plan that includes a timeline to address any weaknesses identified in existing electronic banking controls?

PIB Manual

Many potential weaknesses in online banking controls can be addressed by turning on Personal Internet Branch ("PIB"). However, a credit union may justifiably choose not to employ some or all of these controls based on the preferences of the membership.

17

Does management have documentation to support that it is working with any applicable technology service providers to implement the action plan for compliance?

Idea Forms

*CU*Answers encourages all credit unions to submit requests for changes in Online Banking and all other CU*Answers products using Idea Forms, instructions for which can be accessed here:*

18

Has the credit union implemented appropriate authentication solution(s) to protect member accounts consistent with LTCUs 05-CU-18 & 11-CU-09?

FFIEC Whitepaper

These requirements track the FFIEC requirements:

19

Is the authentication solution required for all member accounts?

Yes

20

Are any identified high-risk accounts and/or transactions protected by layered security controls?

FFIEC Whitepaper

These requirements track the FFIEC requirements:

21

Do layered security controls include anomaly detection and response:

21a

At initial login?

Abnormal Activity Monitoring

There is no anomaly detection at login; however, credit unions can monitor abnormal activity through the use of this menu:

21b

At initiation of funds transfers to external parties?

Easy Pay

Both iPay and Fiserv EasyPay options have fraud prevention options:

FFIEC Authentication Guidance

22
Does the fraud detection and monitoring system consider customer history and behavior to enable a timely and effective response by the credit union?
Yes to all

23
Is there a monitoring process for account maintenance activities?

Abnormal Activity Monitoring

There is no anomaly detection at login; however, credit unions can monitor abnormal activity through the use of this menu:

24
Do layered security controls include simple device identification and/or basic challenge questions?
At the option of the credit union

25
Has management considered the additional layered controls outlined in the Supplemental Guidance?
At the option of the credit union

26
Does the electronic banking system utilize challenge questions as part of the authentication solution? If no, skip questions 24 [sic] a&b.
At the option of the credit union

26a
Has management reviewed the challenge questions and implemented sophisticated challenge questions?
At the option of the credit union

26b
Does the solution refrain from exposing all challenge questions at the same session?

27
Does the electronic banking system utilize device identification? If no, skip questions 27 a&b.
At the option of the credit union

27a
Does the device authentication solution utilize cookies not susceptible to copying?
Yes

27b
Does the device authentication solution creates a complex digital "fingerprint" by looking at a number of characteristics?
Yes

28
Does the credit union have in place a member awareness program to educate members against fraud and identity theft?

Security Grand Opening Kit

*If not, the credit union should launch such a campaign on no less than an annual basis. CU*Answers can help:*

29
Does the credit union offer commercial deposit accounts? If not, skip the remainder of this section, the FFIEC authentication review is complete.
At the option of the credit union

30
Do commercial accounts include a multifactor authentication solution?
Yes

31
Has management considered the layered controls outlined in the Supplement's appendix?

Personal Internet Branch

Through Personal Internet Branch ("PIB"):

32
Do commercial accounts controls include multiple user account profiles?

FFIEC Whitepaper

These requirements track the FFIEC requirements:

32a
If yes, do transaction audit logs identify the user account which performed the transaction?
At the option of the credit union

Mobile Banking

33

Does the credit union provide mobile banking services to members? If no, skip this section.

Mobile Banking Guide

*CU*Answers offers mobile banking which is very similar to Online Banking in controls and use:*

34

Has management performed a documented risk assessment prior to implementing the mobile banking service(s) offered?

No material difference with Online Banking

35

Is there an authentication solution in place to address FFIEC authentication guidance?

No material difference with Online Banking

37

Has management updated the customer awareness program to address mobile banking threats?

Security Grand Opening Kit

*If not, the credit union should launch such a campaign on no less than an annual basis. CU*Answers can help:*

37a

Is the mobile banking provided via an application downloaded to a cell phone or PDA? If No, proceed to question 29 [sic].

No

42

Does the credit union offer an alternate website and/or electronic banking page formatted for mobile devices?

At the option of the credit union

43

If yes, is the mobile site hosted by the same third party hosting the regular site?

Yes

Bill Pay Controls and e-Statements

50
Does the credit union have a written Bill Pay Procedure Manual that provides guidance to employees?

Easy Pay Brochure

*CU*Answers offers Easy Pay through either iPay or Fiserv. Both service providers offer manuals on getting started:*

51
Has management reviewed and adjusted the default bill pay limits?
At the option of the credit union

52
Do members have to submit a request to be enrolled?

Easy Pay Enrollment

This screen will demonstrate how to enroll members into EasyPay; at the option of the credit union, members may enroll themselves

52
Do members receive a Bill Pay Agreement which details their responsibilities and rights for using the system and all required consumer compliance disclosures?
At the option of the credit union

53a
Is access to the bill pay solution provided to the member after they sign-in to the online banking?
Yes

55
Are bill pay transactions reviewed and reconciled daily?

Balancing Made Easy

This document explains reconciliation processes, including Bill Pay

56
Does the credit union offer e-Statements?

Getting Started with e-Statements

This document describes the process for setting up e-Statements

57
Do members have to submit a request to be enrolled?
Yes

58
Is the email address provided by the member validated to complete the enrollment process for e-statements?
Yes

59
Are members notified by e-mail that e-statements are available for review?
Yes

60
Do members receive an agreement which details their responsibilities and rights for using the system and all required consumer compliance disclosures?
At the option of the credit union

Account Aggregation Controls

61
Does the credit union offer account aggregation services to members?

See Jump Controls

*CU*Answers offers account aggregation through See/Jump:*

62
Is the account aggregation service provided by a third party vendor?
Yes

62a
Is there a contract in place with the account aggregation providers which addresses:
Yes, per the Master Services Agreement

62b
Liability of the credit union and provider?
Yes, per the Master Services Agreement

62c
Statement processor will remain in compliance with legal and regulatory requirements?
Yes, per the Master Services Agreement

62d
The authentication and verification process
Yes, per the Master Services Agreement

63
Do members have to submit a request to be enrolled?
Yes

64
Do members receive an account aggregation agreement which details their responsibilities and rights for using the service and all required consumer compliance disclosures?
At the option of the credit union

Hosted Internet Banking

66
Does the credit union host the internet banking application internally? If no, skip this section.
*As to CU*Answers, see below*

67
Is the application hosted on a server in a Demilitarized Zone (DMZ)?
Yes

68
Are there design controls in place which construct and test changes to the software in a test setting?
Yes

69
Have unnecessary services on the web server been disabled and appropriate controls implemented?
Yes

70
Does the credit union obtain penetration tests and regular security scans of the Internet Banking network?
Yes

71
Are login pages for Home Banking/Bill Pay SSL encrypted?
Yes

72
Does the credit union accept new members through the Internet or other electronic channels?
n/a

74
Are member account numbers masked on web pages?
Not shown

75
Does the webpage display the date and time of the last good and bad log-in attempts to the account?
*Yes, reviewed in CU*BASE*

76
Are internet banking passwords maintained at the credit union?
No

80
Can members change their contact information or other critical information via internet banking?
Yes

81
If yes, does the credit union contact the member using both the old and new contact information to verify the information changed via internet banking was performed by the member?
Available

82
Does the website display a warning against unauthorized access to internet banking?
At the option of the credit union

83
Are invalid login attempts logged?
Yes

84
Are policies and procedures documented to provide employees with guidance?
*Yes, as to CU*Answers*

85
Does management maintain a complete list of employees who access or manage the system and the duties each performs?
Yes

86
Are appropriate controls in place for personnel with electronic banking duties (manage/access the system)?
Yes

87
Is administrative access limited to those employees who need access based upon their job description?
Yes

88
Are employee privileges only granted for functions that match their job duties?

89
Are strong passwords required for E-banking administrative platforms?
Yes

90
Does each user of E-banking administrative platforms have unique credentials (i.e. no shared user IDs or passwords)?
Yes

91
Are administrative logs reviewed by a supervisor and audited periodically?
Yes