Completing Your Credit Union's

Internet Banking Risk Assessment

Revised: **June 21, 2011**

Introduction

Ever since the original "Guidance on Authentication in Internet Banking Environment" was distributed by the NCUA (letter 05-CU-18), credit unions have been aware that they need to complete a risk assessment of authentication practices as they relate to Internet banking products.

There has been much marketplace confusion around this topic, from, "you have to buy something right now" to, "this is much ado about nothing." This has also caused many conversations about the best way to do a risk assessment, and what truly needs to be done. As recently as August 8, 2006, the NCUA posted additional information for credit unions to consider as part of their risk assessment responsibilities (see NUCA letter 06-CU-13, available at http://www.ncua.gov).

Our goal with this document is to provide our viewpoint, as the provider of **It's Me 247** Internet banking, on the risks associated with providing this particular Internet banking service to your credit union's members.

The reason we are doing this is that our CUSO has always worked as a peer network, and when possible, by proxy. Ever since the Y2K and Managing e-Commerce projects, CU*Answers has established a track record for taking part in responding to regulatory and marketplace mandates.

As with those efforts, it is our intention to provide you with technical information, explanations, and business considerations you can use to help you with your own risk assessment. Remember that CU*Answers can only provide advice and input into the process. Your credit union is still responsible for doing the actual assessment of the risks that your members face when they choose to use the Internet banking products your credit union offers. This includes **It's Me 247**, of course, as well as any other Internet-based products you have made available to your members, such as online access to a brokerage service or a third-party A2A service.

Remember, you must present your risk assessment and be ready to defend it as part of your business plan in the future.

> Now for the fine print: Like the disclaimer you might see at the beginning of a television program, any opinions expressed in this document are just that, opinions from CU*Answers technical, security, and management teams. They are not intended to be a substitute for careful review and assessment by a credit union representative.

Assessing the Risk

What does "risk" even mean?

In black and white, the guidance says you have to decide whether something is "high risk" or not. The side of us that is analytical, cautious, and wants to get it right no matter what, says, "Okay, tell us what is high risk? What's the right response?"

Unfortunately, this is not one plus one equals two. This is not a mathematical equation that clearly has a right answer for everyone. This is about your opinion and how your organization balances the uniqueness of what you offer, the uniqueness of how your members use it, and the uniqueness of your goals for the future.

The biggest new wrinkle with today's members is that they are not homogenous. (They probably never were, but for far too long, our industry has treated them as if they were.) They don't all think the same, and they don't all react the same. So you have to balance your decision by considering where you are as much as where you hope to go. Be careful not to use too narrow a viewpoint when you think about risk. It can narrow your opportunities.

For that reason, you must consider your experiences as to past losses and your realistic forecasts for future losses. Make sure the medicine doesn't kill the patient by spending big bucks for solutions to problems that have no real potential for losses. In this situation, overestimating the potential losses related to risk will sink your opportunities.

Regulations have a tendency to group everyone into the same mold. They imply all members are doing the same things on the Internet, that all financial institutions have the same goals on the Internet, and that all of our business plans are consistent. It is the nature of the beast. Every leader must resist jumping to conclusions, and take the track that best fits an individual approach to applying regulations.

4 Key Areas of Risk

We see four main risk areas related to Internet banking services:

Risks to Members	*Risks to Credit Unions and CU*Answers*
1) That Internet Banking would cause a member to lose **money** directly (i.e., check withdrawal or transfer to other person)	That security will become too expensive or complicated and therefore:
2) That Internet Banking would allow someone to capture member **personal identity** information	**3)** Members will choose not to use credit union Internet products
	4) Credit unions will elect not to use CUSO Internet products

Without a doubt, the biggest risk to credit unions is that we would be locked out of the Internet self-service financial service industry in the future—either in the minds of our members, regulators, or ourselves.

Tools To Help You Assess It's Me 247 Risk

Overview of It's Me 247 Security Features

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 and password combination known only to the member. Members can select to create a Username to be used in place of the account number. Without this information, accessing account data and initiating transactions online is impossible. 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 (six to ten characters is recommended, with six characters being required). 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.

It's Me 247 Product Feature Matrix

To help you assess the specific risks related to **It's Me 247**, we have developed a Product Feature Matrix that lists all of the features that can be activated for **It's Me 247**.

Next to each feature is noted whether that specific feature or page on the **It's Me 247** website contains information that might present one of the two member-related risks:

1) Risk to member money, or
2) Risk to member identity.

In addition, **It's Me 247** already contains many features that are specifically designed to add and enhance security for members. These features have been noted on the matrix. Many are configurable and can be activated or adjusted by your credit union.

> **Is your credit union taking advantage of these existing security features**, especially those that pertain to expanded passwords? Refer to the "Strategies for Controlling Member Access to **It's Me 247**" document (attached) for more details.

Following is a list of the key expectations outlined in the Guidance, with some tips on how to use the Matrix as you approach the portion of your risk assessment that relates to **It's Me 247**:

What does the NCUA expect?	*CU*Answers suggestions for completing the portion of your risk assessment related to **It's Me 247**...*
Identify all transactions and access associated with Internet-based products and services (that includes, *but is not limited to*, **It's Me 247**)	■ Review the attached **It's Me 247** features matrix, marking out any items that your credit union does not offer at all
Determine if any of the transactions in that list are considered by your credit union to be high risk	■ Examine the remaining features on the matrix and mark any you consider to be high risk
Identify authentication methods currently used for Internet-based services	As described in the "Overview of **It's Me 247** Security Features" discussion above, **It's Me 247** uses single-factor authentication (account number and PIN/password) with configurable options as to password length, non-use expiration, restricted password retries, and whether the password is used for both **It's Me 247** and CU*TALK. ■ Review both the attached Product Feature Matrix as well as the "Strategies for Controlling Member Access to **It's Me 247**" document to better understand existing **It's Me 247** security features.
Determine effectiveness of authentication methods for high risk transactions	■ Think about the tasks you marked as high risk; do you consider the current **It's Me 247** authentication features to be adequate?

Mitigating Risk

Tools You Already Have to Control Risk

Remember that not all of the features and tools listed in the Matrix are automatic - many of them are optional and must be specifically activated by your credit union. For example, the ability to apply for a loan online must be configured and activated by your credit union before it is even available. Other features, such as the ability to view cancelled check images or the controls that determine whether or not members can transfer funds outside of their own account, are also credit union-defined.

This means that you have already been making decisions about whether a transaction type is risky, simply by choosing whether or not to offer the feature in the first place. If your credit union worries that the ability to view check images online is risky, one way to mitigate that risk is simply to deactivate the service. Of course, that depends on how important that feature is to the other risk area: whether members will choose to use the online banking product at all if that feature is not available to them.

Developing Credit Union Policies and Procedures to Mitigate Risk

In addition to activating optional features and tools in online banking, your credit union also mitigates risk by the way it sets policies and procedures related to offering and supporting online banking services for members:

- How do you manage **resetting passwords** for members? *How do you authenticate a member who calls on the phone asking for his password to be reset? Who can handle a reset? Are resets logged? Can a member ask an MSR to enter a specific custom password for them over the teller line? (Yes, there is a CU*BASE configuration feature that controls whether that feature is available or not!)*
- What are your policies and procedures for how online banking is implemented for **new memberships**? Does every new member get it by default, or do you have a monitored signup process? *(Refer to the "Strategies for Controlling Member Access to **It's Me 247**" document for some tips.)*
- Do you have policies for **expiring passwords** when members don't use online banking regularly? *(Refer to the "Strategies for Controlling Member Access to **It's Me 247**" document for tips about expiring passwords for inactive members.)*
- Is online banking access covered in your **dormancy** policies and procedures?
- What is your approach for how members **move money** on the Internet? *How will you configure **It's Me 247** to manage money movement, whether it be internal to the membership, from one member to another, or in the future, between financial institutions?*

  More than just share to share transfers, we're also talking about disbursing loans to checking accounts or the way people make payments. Having a comprehensive plan that can evolve with new technologies related to money movement is important to your annual risk assessment. CU*Answers also offers Account-to-Account services. (A2A relationships must be set up by a Member Service Representative before they are available in **It's Me 247** for transfers.

- What is your approach to how members **manage their identity** on the Internet? *How do you feel about options that identify who they are (address maintenance), who they do business with (bill pay or AFT), or where their direct deposits come from (ACH)? Having a strategy that allows members to do these things but also protects the way they do it is important. Do you have a plan for how members opt out of these functions?*

Remember, it's not just the tools you use (**It's Me 247**); it's the strategies that set the tone for where you are going with Internet services. It's the behind the scenes, people things in your office that create the overall Internet risk you have. For example, is it easy to talk to a credit union employee and have your password reset without identifying yourself? This isn't technical, this is social.

New Tools Offered by CU*Answers

If the conclusion of your risk assessment is that the standard level of authentication for **It's Me 247** Internet banking is inadequate for the high risk transactions you have identified, and your *business* evaluation says you still need to offer that feature to make online banking valuable to your members, you must decide which authentication method your credit union will plan to add.

Remember that you only need to implement <u>one</u> of the following; you do NOT need to implement all of them. (And you don't need to add *any* of them unless you determine the existing authentication controls are not adequate according to your assessment of risk.)

Recommended Authentication Methods	*CU*Answers Solutions for **It's Me 247**...*
Layered Security	Activate the optional **PIB** (Personal Internet Branch) layered security feature to allow members to control access to their own specific account through **It's Me 247**. Includes controls by feature, day of week, time of day, and even geographic location. It layers additional passwords and member authentication internal to **It's Me 247**. *See the "Introducing PIB" presentation for more details.*
Multifactor Authentication	Throughout 2006 CU*Answers has diligently been reviewing token strategies with multiple partners. Based on lukewarm interest from our current credit unions to move too quickly in adding this expense to their programs or additional inconvenience for their members, CU*Answers has not made a final decision on which solution to choose. We do believe that credit unions with aggressive programs (investment management, A2A, etc.) will have an audience for tokens (5% of online banking users). Based on the response of CU*Answers owners and clients, and the plans they put forward through their risk assessments, CU*Answers will respond quickly in the first half of 2007. *This strategy is based on a shared CUSO investment in setting the foundation for tokens. Should a CU deem it immediately necessary to add tokens to their program, CU*Answers will work directly with that credit union on the investment they need to make.*
Other Controls	This is the NCUA's way of allowing for "*technology and controls that are emerging or that may be introduced in the future*." That means it is a wildcard that will be monitored and evaluated on an ongoing basis by CU*Answers technical and security teams.

Educate, Educate, Educate

CU*Answers believes that every risk assessment will come to the same conclusion about the number one thing to do related to the risks of the Internet: we must educate members to use the channel effectively. This is not optional; this is the best insurance that the credit union and CU*Answers have done the prudent thing on the member's behalf.

Beyond safety labels, warnings, or disclaimers, this education program needs to be a proactive, best-practice, recent-events type of effort. In the end, everyone benefits. The financial institution develops a clearer strategy for defining value, encouraging usage, and growing their program. The member gains a trusted partner and a center for learning about the best ways to participate with these products.

This is both a top down and a bottom up strategy. Everyone must be involved in the effort. We must market the education program as being available instead of just passively placing it on websites, intranets, or brochure racks. We must be able to prove to the regulator and to ourselves that we have done everything possible to give the member the edge.

Get involved with Partners in Practice and the CU*Answers Web Services teams. Look for new announcements by Member Reach on a proactive member contact program to keep your members in touch with new educational tools.

Continuing Your Risk Assessment Program

The easiest thing to do is to say that you are going to review this annually, that once a year you will check off that your risk assessment is done and your program is just fine. One more task on a static checklist. We all do it; it's a common trap. CU*Answers has not been immune to this kind of thinking in the past, either.

Just as the security environment is constantly changing and evolving, so must **It's Me 247**, and so will the business considerations and technical details covered in this document. CU*Answers knows that we must make assessing risk, responding with strategies, and staying on top of where members are going on the Internet a day-to-day cultural response instead of an annual task to check off our list. We encourage you to do the same. Update your risk assessment and your business plans related to the Internet frequently and based on participating in multiple events such as focus groups, educational opportunities, and networking with your peers.

A message to credit union leaders...

I've talked to a lot of credit union leaders around the country since this issue hit the headlines. I've talked to CEOs who said, "It's no big deal. You simply pick a tool that is cheap enough to keep the regulators off your back, and move on." I've talked to leaders who said their Internet strategies were still developing and still new enough that they couldn't afford any more expense and continue to profit when balancing all their other initiatives. I've even talked to leaders who said, "This is why we don't push the Internet, and we probably never will."

There are a lot of opinions about this. But the group that makes me sit up and listen are the leaders who say, "My members are going to do their personal finances on the Internet, no matter what. They've made the decision to work through the issues related to financial risk, identity risk, or whatever other risks there are. This is no different from getting in your car and assuming the risks in driving down to the branch. They're going to do it. Therefore I must have a strategy that is as forward-thinking as my most progressive members are, that is convenient and easy to use, and that puts them in the driver's seat."

This is why we are developing the PIB profile. Members can select the security tools they wish to use, pick the transactions they think are important, and define how and when they use credit union Internet services. We must be prudent in protecting our organizations, and the most prudent thing we can do is to empower the member and to be relevant to their life.

Make sure your program considers members one on one. Trust what they want, and trust that if you don't provide it, it does not mean they will not go and find it somewhere else.

Randy Karnes, CEO
CU*Answers

Requesting an Electronic Copy of this Document

If you would like an electronic copy of the Risk Assessment or any of the materials listed here, visit our website at **www.cuanswers.com/security**.

Feel free to copy, append, modify, and use these documents in any way you wish to assist your credit union in developing its own risk assessment.

Packet Contents

- **It's Me 247** Risk Assessment: Product Feature Matrix
- Strategies for Controlling Member Access to **It's Me 247**
- Introducing PIB: A Personal Internet Branch for Credit Union Members
  (PowerPoint presentation used during the 2006 Annual Leadership Conference)
- Presenting Your Personal Internet Branch
  (Sample marketing piece: tri-fold brochure)