

Answering Your Questions About PIB

Revised December 07, 2007

You've completed your latest Internet Banking Risk Assessment process, have you? If your assessment has concluded that you need to implement additional authentication features for **It's Me 247**, now what? That's where PIB comes in.



So Just What is PIB?

PIB provides a **layered security approach** to add additional authentication controls and member personalization features to **It's Me 247**. PIB, which stands for Personal Internet Branch, is an independent application that provides multiple, configurable controls that govern how online banking behaves and what members can do in online banking.

PIB allows your members to control access to their accounts with controls by feature, day of week, time of day, and even geographic location. It layers additional passwords and member authentication internal to online banking.

Your credit union can configure default PIB settings for your members, and you can even decide just how much control you want your members to have in managing their own settings.

CU*Answers designed PIB to go far beyond just complying with the latest regulatory expectations and provide some real value to your members. It's a powerful feature. It does some really cool things. It's something new and probably very different from what most of your members have ever seen before.

But with that power comes necessary complexity and the need for careful consideration. Make sure you go in with your eyes wide open.

Why Use Layered Security?

A bad guy somehow gets your online banking user name and password. What can he do while he's there? The more controls you have in place, the less that bad guy (or gal) can do to hurt you.

Of course you must balance the relative safety of disabling access against your convenience in doing what you want to do with your accounts.

Imagine if you put a different lock on every door in your house and locked them all, all of the time. Even if a burglar managed to get in your front door, he would be thwarted every time he tried to go into one of the rooms. However, it would make living in your house very inconvenient for you and your family.

So you weigh these two extremes and come up with something in the middle. On your house, you make the front door very difficult to enter, and you put your valuables in a safe with a combination lock. Online, you set up controls that make it difficult for someone other than you to log in, then you put extra locks in place by deactivating certain features or requiring a second password wherever you want extra protection.



Other Tools You Should Be Using to Control Risk

Remember that your credit union's responsibility for mitigating risk doesn't stop when you flip the switch to turn on PIB. Your policies and procedures related to offering and supporting online banking services for members are just as important.

Make sure you have also considered:

- **Your password controls and education program.**
Are you still using the same PIN for audio response and online banking? Now is the time to implement that change, regardless of what your plans are for implementing PIB. Will you enforce strong passwords for **It's Me 247** and educate members on the importance of keeping passwords secure?
- **How you manage resetting passwords for members.**
How do you authenticate a member who calls on the phone asking for his password to be reset? Is the member's identity carefully verified? 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!)
- **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 separate "Strategies for Controlling Member Access to **It's Me 247**" document for some tips.)
- **Policies for expiring passwords when members don't use online banking regularly.**
This should be part of your dormancy monitoring policy. (Refer to the "Strategies for Controlling Member Access to **It's Me 247**" document for tips about expiring passwords for inactive members.)
- **How online banking access is covered in your dormancy policies and procedures.**
- **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. How might the risks change if CU*Answers was to include A2A (financial institution to financial institution) transfers in the future?
- **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. How easy is it for someone to call a credit union employee and have a password reset without identifying themselves? This isn't technical, this is social.

What Features Does PIB Control?

Following are the security and personalization features that can be activated for each member through their PIB Profile:

- Log in to **It's Me 247** via username instead of account number
- Knowledge-based challenge questions to log in to **It's Me 247**
- Control access to **It's Me 247** by:
 - Geographic location (IP address when logging in to online banking)
 - Computer (persistent cookie stored on member's computer)
 - Day of week
 - Time of day
- Control access and/or add additional confirmation code for certain **It's Me 247** transactions, including:
 - Transfers
 - Check withdrawals

- ACH deposit maintenance
 - AFT/CFT record maintenance
 - Apply for loans
 - Open checking/savings accounts
 - Open certificates
 - View cancelled checks
 - Manage personal information (address, phone number, email address, etc.)
 - Manage online bill pay
- Set up inter-member transfer control lists online (via PIB Profile web tool only)

Answers to Your Questions

Q: Is PIB the same as multi-factor authentication?

A: No. PIB is a **layered security solution**, which is one of the three methods recommended by the NCUA to comply with the “Guidance on Authentication in Internet Banking Environment” (letter 05-CU-18). Remember that you only need to select one of the three available methods. (The other two methods are multi-factor authentication, and “other controls,” the NCUA’s way of allowing for technology that doesn’t even exist yet.)

Although the term “multi-factor authentication” is sometimes misused and often misunderstood, what most people mean is actually two-factor authentication:

Factor One: Something You Know (*a username, password, PIN, etc.*)

Factor Two: Something You Have (*a USB token that generates passwords, a fingerprint, a dongle, a smart card, etc.*)

Two factor authentication generally requires customers who want to log into their accounts online to use a username and password (single factor authentication) and a small token that generates a new password every minute or so (two factor authentication).

In 2006 CU*Answers began 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 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.

Q: I heard someone in the industry say that dual authentication is mandated by FFIEC for anyone doing high risk transactions, like bill pay and moving money to another account. Who’s right?

A: Here’s what NCUA letter 05-CU-18 says:

“You should identify and evaluate the risks associated with the Internet related services you provide for your members...

“Where the risk assessment indicates that the use of single-factor authentication is inadequate for the types of services period *[sic]*, you should employ multifactor authentication, layered security, or other controls.”

So yes, if your risk assessment says that bill pay and moving money to other accounts are high-risk transactions, then you have to implement an additional authentication method. That means multifactor, or layered, or other controls.

Q: Do I have to turn on PIB right away?

A: No! **It's Me 247** will continue to work just fine whether you decide to activate PIB or not.

In fact, you should not activate a change this significant without some careful planning and preparation. You need a plan. A plan for marketing the change to members. A plan to train your staff. A plan for rolling out the changes with an acceptable level of disruption to members and staff. A plan to handle the increase in phone calls and frustrated members. A plan to make this part of your process for opening new memberships. A plan for ongoing marketing and reinforcement.

Remember that if your risk assessment indicates that no new authentication methods are needed right now, you can spend some time deciding whether PIB is right for you, then flip the switch when the time is right.

Q: Can I just turn off features that I think are high-risk?

A: Actually, yes. And you could always do this. Features such as inter-member transfers, AFT/CFT maintenance, and personal information update have always been optional features you can deactivate. Depending on your members' needs, this may be a viable option to reduce the risk of offering online banking to your members. The key phrase here is, "your members' needs." Simply turning off features you think are risky doesn't mean your members won't still need to do those things.

Q: Can I turn on PIB but make it more "transparent" to reduce the impact?

A: There are a couple of ways you can plan your rollout to reduce the immediate impact on members. In fact, a phased-in implementation method will be the best way to go for any credit union. *Watch for more information about setting up a complete rollout plan, coming soon!*

Q: What if my members don't want to set up a PIB profile? Is there a default profile we can set up for them?

A: Yes, your credit union can set up a default PIB Profile for all members. This includes things like requiring knowledge-based challenge questions to log in to **It's Me 247**, on/off flags for individual features, and maximum transaction amounts. This is in addition to the controls you already have related to **It's Me 247**.

Be aware that the default settings are limited to those controls that don't require the member to make a decision. For example, features such as persistent cookies and geo-location tools must be initiated by the member using his or her actual computer. As another example, there is a feature that allows for a secondary password, called a confirmation code, to be required for certain types of transactions. Since the member needs to set up that code, that requirement won't be part of your default, but you could still make it part of your procedure when setting up a new profile with a member. The point is that depending on what controls you want to specify as the default, you may still need to get the member involved at least by talking with a CU representative to complete certain settings.

Q: Will it cost me anything to turn on PIB?

A: Well, CU*Answers won't charge you any fees to use the PIB system for your members, and there is no up-front implementation cost. If members use the online tool to adjust their PIB Profile, that will not be counted toward your **It's Me 247** usage minutes. So yes, PIB is "free," at least as far as the line items on your CU*Answers invoice go. But as we've already stated, you will need to plan for increased staff training time, increased phone support for your members, changes to internal procedures such as opening new memberships, and ongoing marketing and education efforts.