CU*BASE AND THE FFIEC SUPPLEMENT TO AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT

Your Guide to Compliance

Introduction

Financial institutions are now at an increased risk for liability if consumer funds are stolen electronically. Even if the consumer is partially negligent by using their account insecurely, the financial institution can still be held liable if the transactions processed are suspicious.

The Federal Financial Institution Examination Council, or FFIEC, has recently issued a Supplement to their Guidance to Authentication in an Internet Banking Environment ("Supplement"). *The NCUA has declared that all credit unions will be tested against this FFIEC document by 2012.*

All financial institutions processing online transactions need to be aware of the risk and how to defend their members against electronic theft. CU*BASE offers every credit union that processes online financial transactions the power to configure transactions to safeguard member assets and move towards compliance with the new regulatory requirements. By following these best practices, a credit union can not only help protect their members from online theft of funds, but also protect themselves from liability should a member's funds be stolen electronically.

Contents

The Five Part Checklist for Online Banking Compliance

In order to meet the new compliance requirements, every credit union should follow these five steps:

Step One: Conduct a Risk Assessment on All Online Banking Accounts

If the account involves large dollar amounts passing from the credit union to outside third parties, the risk should be considered **high**, and the credit union should act accordingly.

Step Two: If Commercial, Set Administrative Functions

Business accounts should have enhanced controls for system administrators who have privileges for setting access, configurations, and limits.

Step Three: Set Layered Security

Depending on the risk level of the account, set up access and authorization controls, and set thresholds for account activity including transaction value thresholds.

Step Four: Detect and Respond to Suspicious Activity

CU*BASE is undergoing development to provide each credit union with the tools to monitor the transaction history of members to allow analysis of suspicious activity. These features will be available in 2012.

Step Five: Customer Awareness and Education

At least annually, advise your members on how to protect their accounts, and provide regular follow-up on new threats or ways to enhance the security of their online banking activity.

Step One: Conduct a Risk Assessment on All Online Banking Accounts

The two key factors a credit union should keep in mind when assessing the risk of online banking is whether the funds can be taken out of the account and how much money is actually at risk. *Credit unions should be careful not to process online transactions to outside third parties that are greater than the credit union is willing to lose*. Once funds are out of the credit union's control, the ability to recover those funds is minimal.

Rules of thumb to consider when assessing risk include the following:

Transaction Amounts	Destination	Risk
The transaction amounts are large (such as commercial accounts)	To outside third parties, such as A2A or Online Bill Pay	Should be considered **HIGH**
The transaction amounts are small	Small transactions to outside third parties, or larger transactions to parties within the credit union	Should be considered **MEDIUM**
The transaction amounts are small	The transactions are within the same accounts of the member (e.g. savings to checking) or the possibility of loss is minimal	Should be considered **LOW**

The FFIEC Supplement states financial institutions are *required* to do risk assessments on the following basis:

- New information regarding threats to online accounts is available.
- New online financial services are being offered.
- No less than every 12 months.

All credit unions should perform this analysis when opening an account. For existing accounts, credit unions can use **Tool #774: *Sample Checking Account Activity*** to analyze the riskiness of the accounts. In addition, credit unions can use Due Diligence codes to assign risk scores to accounts that engage in online banking. As part of a credit union's compliance analysis, all online banking risk assessments for existing clients should be completed by 2012.

SecuriKey CU*Answers offers the SecuriKey documents to give you quick access to the answers you need for your due diligence requirements. Find the SecuriKey Risk Assessment for Online and Mobile Banking on the CU*Answers Risk Assessment Center page: https://www.cuanswers.com/resources/risk-assessment-center/. (Look for the SecuriKey logo.) The Guide gives an overview of the important features of the product, and how to access additional information and services relating to the product. This is an excellent document to provide to examiners.

Step Two: If Commercial, Set Administrative Functions

The FFIEC wants financial institutions to take additional care when it comes to commercial online banking accounts. Credit unions need to ensure that business accounts have additional controls when setting up system administration functions.

Credit unions can manage these controls by using PIB (Personal Internet Branch). PIB allows credit unions to set a large range of controls regarding the personnel authorized to make changes, what activity can be done online, and in what amounts. PIB is the primary system for protecting both the member's funds and protecting the credit union from liability. Other "Layered Security Controls" also allow you to remain in compliance. Refer to the "Layered Security Controls" section (starting on page 10 of this document) for more complete information on PIB and the other security options for your credit union. This section is referenced in the table below.

NOTE: Credit unions may wish to maintain control of PIB functions rather than allow the owner of the commercial account to make changes. By controlling PIB from within the credit union, the credit union reduces the risk that unauthorized personnel are making changes to the online banking security settings.

The three main controls that should be set for commercial online banking accounts include:

Control	Purpose	Compliance Tools
Email notification	Members must always be notified when there is an administrative change to online banking; confirmation emails may need to go to someone other than an authorized user	• Email notifications are sent when any change is made to the member's contact information via online banking. Email change notifications are sent to both the old and new email address. *See Personal Information Change on page 13.* • If a change is made to a PIB setting, the member receives an email notification. *See Personal Internet Branch (PIB) Controls on page 14.*
Confirmation codes	Requires a confirmation code before a high-risk transaction can be performed	• PIB can require the entry of a confirmation code before transaction activity is allowed in online banking. *See Personal Internet Branch (PIB) Controls on page 14.*
Password changes	Should always be through the credit union, including changes to confirmation codes	• Member education is needed by the credit union since members have the ability to change their passwords via online banking. • Members receive emails notifications for all online banking password changes. *See Password on page 12.* • Members receive email notifications for all PIB confirmation code changes. *See Personal Internet Branch (PIB) Controls on page 14.*

Step Three: Set Layered Security

Layered Security is a term meaning that a credit union should have multiple controls with respect to online banking so that if one control fails another prevents or mitigates the damage. For example, if a criminal is able to obtain a member's online credentials, layered security that includes dollar limits on the amounts that can be stolen helps mitigate the damage that the criminal can cause. The PIB (Personal Internet Branch) system allows the credit union to set up layered security for each and every online banking account in accordance with the new FFIEC Guidelines. Other "Layered Security Controls" also allow you to remain in compliance. Refer to the "Layered Security Controls" section (starting on page 10 of this document) for more complete information on PIB and the other security options for your credit union. This section is referenced in the table below.

*NOTE: PIB should now be considered a **requirement** for any member engaging in high risk online banking activity. Credit unions can select to restrict PIB controls and also to select to edit the PIB settings of selected accounts. Alternatively credit unions can allow members to set their PIB settings themselves. This document is written with the expectation that the credit unions will block access for member PIB adjustment, and also that it will set additional limits for high-risk accounts via Member Personal Banker.*

The layered security controls that should be considered for every high risk online account include:

Control	Purpose	Compliance Tools
Set custom/complex PIN and passwords	Should be a requirement for any high risk transactions	Credit unions can select to activate complex passwords. *See Password on page 12.*
Email notification for password resets	Members should receive an email notification each time their password is reset	Members receive an email each time their online banking password is reset. *See Password on page 12.*
Email notification on password change	Members should receive an email notification each time their password is changed	Members receive an email each time their online banking password is changed. *See Password on page 12.*
Email notification for contact information changes	Members should receive an email notification each time a change is made to the contact information of an account, such as physical address or email address.	Members receive an email notification each time their contact information is changed, including email and physical address. *See Personal Information Change on page 13.*
Transaction dollar limits	Critical in high risk transfers to outside third parties	Transaction dollar limits for transfers (including A2A transfers) can be set for transactions via PIB. *See PIB on page 14.*
Transaction time limits	Restricts when transfers can take place; useful for businesses who do not need 24/7 online banking access	The hours when a member can access online banking can be set via PIB. *See Personal Internet Branch (PIB) Controls on page 14.*
Confirmation codes	Further protection when performing a transaction online	PIB can require a confirmation code for online banking transfers and other transaction related activities. *See Personal Internet Branch (PIB) Controls on page 14.*
Control	**Purpose**	**Compliance Tools**

Disable unused transactions	Credit unions should disable all transactional activity not required by the consumer	Certain transaction related activity can be disabled via PIB. This includes access to bill pay and to Check Funds Transfer, which allows the sending of a check to another person. *See Personal Internet Branch (PIB) Controls on page 14.*
Transfer Control Lists	Requires that members are only allowed to transfer to a controlled list of members	Members can only transfer to memberships on their Transfer Control List. This not only includes transfers made via the Transfer Wizard, but also online banking transfers made via the ACH Distribution and Automated Funds Transfer (AFTs) features. Credit unions control the addition of memberships to this list. *See Transfer Control Lists on page 17.*
Account-to-Account (A2A) Controls	Places controls on A2A transfers for high risk accounts, or blocks members from its use entirely	Members must set up an A2A Relationship before they can transfer to an account of an outside financial institution. Credit unions control the set up of these relationships. PIB can also block access completely to this feature or control the dollar amount per day of the transfers. *See A2A Controls on page 10.*
Bill Pay	Disable bill pay for high risk accounts or require a confirmation code for access	PIB can disable the use of bill pay in online banking and in Mobile Web Banking. PIB can also require a confirmation code for access. *See Personal Internet Branch (PIB) Controls on page 14. Also review Bill Pay on page 11 and Mobile Web Banking Controls on page 11.*
Mobile Web Banking Controls	Determines which activities are permitted via Mobile Banking	Transfer control lists are used to determine which memberships a member can transfer to via Mobile Web Banking. PIB can set dollar limits on transfers and access to bill pay. *See Mobile Web Banking Controls on page 12. See also Personal Internet Branch (PIB) Controls on page 14.*
Audio Banking Controls	Determines what activities are allowed over the phone	Members are not allowed to transfer funds to other memberships via audio banking. *See Audio Banking Controls on page 11.*
Controls by Dividend Application	Determines the maximum that can be transferred via audio and online banking by Dividend Application	Determines the maximum amount that can be included in an outgoing transfer via online and audio banking. This includes both transfers within and outside of the credit union. *See Dividend Application Controls on page 11.*

Credit unions should be aware that failure to enable some or all of these controls, depending on appropriateness, greatly increases the chances the credit union will be held liable for processing high risk transactions that turn out to be fraudulent. The administrative overhead of administering these controls is minor compared to the potential risk of liability.

Step Four: Detect and Respond to Suspicious Activity

Because online threats are very effective at compromising even security-savvy consumers, financial institutions now have an obligation to avoid processing suspicious transactions, or suffer the risk of being held liable if suspicious funds transfer ends up being fraudulent. The mere fact that the member's credentials were *authenticated* is no longer a defense to the credit union if the *transactions* were suspicious.

To meet this requirement, CU*Answers is developing toolsets within CU*BASE to allow credit unions to analyze the transaction behavior of members and flag activities that are anomalous or suspicious. With a click of a button, credit unions will be able to track member behavior and see graphically patterns of behavior that are deviant or suspicious. This transactional analysis, combined with a robust layered security program, greatly reduces the risk that a credit union will process or be held liable for fraudulent transactions.

These transactional analysis functions will be available in 2012 in time to meet the new compliance requirements.

Step Five: Customer Awareness and Education

Finally, credit unions must constantly provide educational information to the membership regarding online banking security. Some of the examples that the FFIEC used are as follows:

1. An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access.

2. An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials.

   Note: From a security standpoint, this should be rarely, if ever.

3. A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically.

4. A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found.

5. A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.

Layered Security Controls

This section covers the various controls your credit union can use to you to remain in compliance. Use this Layered Security Controls section in conjunction with the previous **Step 1** and **Step 2** of this document.

Account to Account (A2A) Controls

Credit unions must first select to activate A2A. Contact a Client Services Representative for assistance.

- NOTE: PIB allows you to turn off A2A for your credit union or for an individual membership. PIB can also control the per day dollar amount of transactions made via A2A. See Personal Internet Branch (PIB) Controls on page 14.

Before a member can transfer funds to an outside account, the member must first set up an A2A Relationship at the credit union. (Credit unions must configure A2A Relationships for members in CU*BASE; members cannot do this in online banking.) Once the Relationship is configured, the member can then initiate transfers to that account via the Transfer Wizard in online banking.

Credit unions set up the member's A2A Relationships via Tool #14 ***Member Personal Banker.*** Following is a picture of the screen used to configure the relationship.

A2A Relationship Configuration

- Refer to the Account-to-Account (A2A) Transfers (http://cuanswers.com/pdf/cb_ref/A2ATransfers.pdf) booklet for more complete details on A2A transfers.

Audio Banking Controls

Members are not allowed to transfer funds to other memberships via Audio Banking. Dividend Application configuration can control the maximum transfer amount for transactions within the credit union. *See Dividend Application Controls on page 11.*

Bill Pay

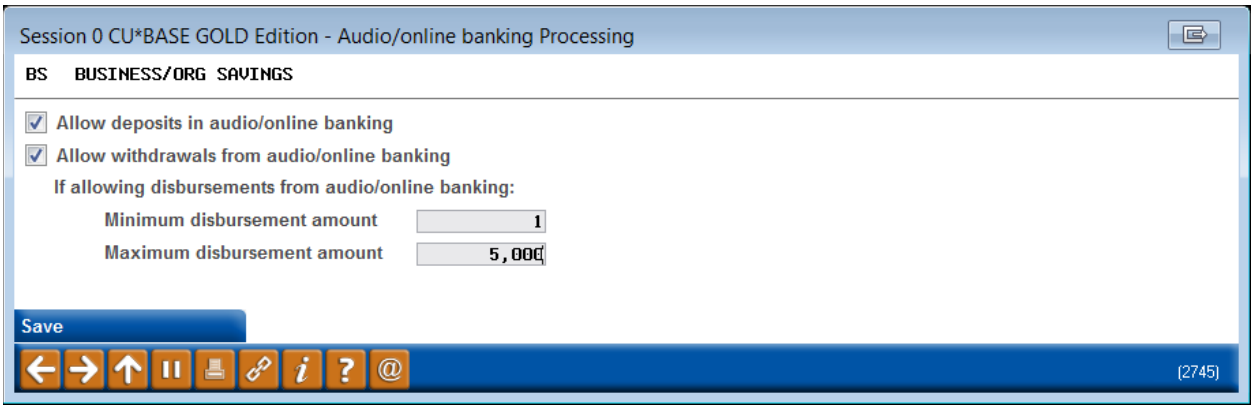
Credit union must first select to activate bill pay. Contact a Client Services Representative for assistance.

The PIB control "Pay bills online" allows credit unions to disable the use of Bill Pay in online banking. Mobile Web Banking also follows this configuration. PIB can also require the entry of a confirmation code for access to bill pay. (This feature currently is only available for access via standard online banking and is not yet implemented for Mobile Web Banking.) *See Personal Internet Branch (PIB) Controls on page 14.*

- Refer to the PIB: Configuration/User Guide (http://cuanswers.com/pdf/cb_ref/PIBConfiguration.pdf). Also refer to the Mobile Web Banking booklet (http://cuanswers.com/pdf/cb_ref/mobilebanking.pdf).

Dividend Application Controls

The Audio/Online Banking controls in the Dividend Application Configuration can control the maximum dollar amount a member is allowed to transfer from online or audio banking. This control is credit union wide (for all membership transfers via audio or online banking) and is configured by selecting **Too1 #777: *Savings/Checking Products Config***. From the product configuration screen select *ARU/Online Banking* (F15).)



Mobile Web Banking Controls

Credit unions must first activate Mobile Web Banking. Contact a Client Services Representative for assistance.

While in Mobile Web Banking, members can only transfer funds to the accounts on their Transfer Controls List. *See the "Transfer Controls List" section on page 17.*

Mobile Web Banking also follows the following PIB controls. *See Personal Internet Branch (PIB) Controls on page 14 for a list of all PIB controlled features.*

- Transfer money within my own accounts
- Confirmation code for transfer within a base account
- Transfer to another base account
- Confirmation code for a transfer to another base account
- Transfer Limits for single transfer to another base account
- Manage Online Bill Pay (allow/disallow the use of)
- Days and Times Available (Limiting Access by Day of Week or Time of Day)

- Refer to the Mobile Web Banking booklet (http://cuanswers.com/pdf/cb_ref/mobilebanking.pdf).

Password

Members are required to create a password of at least six characters (or a number of characters chosen by the credit union). Credit unions can also choose to activate "complex passwords" which requires a member to create a password with three of the following: upper case, lower case, number, and special character. Members receive an email notification and message in the Secure Online Banking Message Center each time their password is reset or changed.

- Credit unions can request to activate complex passwords or to increase the number of required characters in a password by filling out an It's Me 247 Configuration Change Request Form (http://cuanswers.com/pdf/cb_ref/ItsMeCHConfigForm.rtf).
- Refer also to the It's Me 247 Strategies for Controlling Member Access (http://cuanswers.com/pdf/security/ItsMe247PINstrategies.pdf) and Communication with Members (http://cuanswers.com/pdf/cb_ref/communication_with_members.pdf).

Personal Information Change

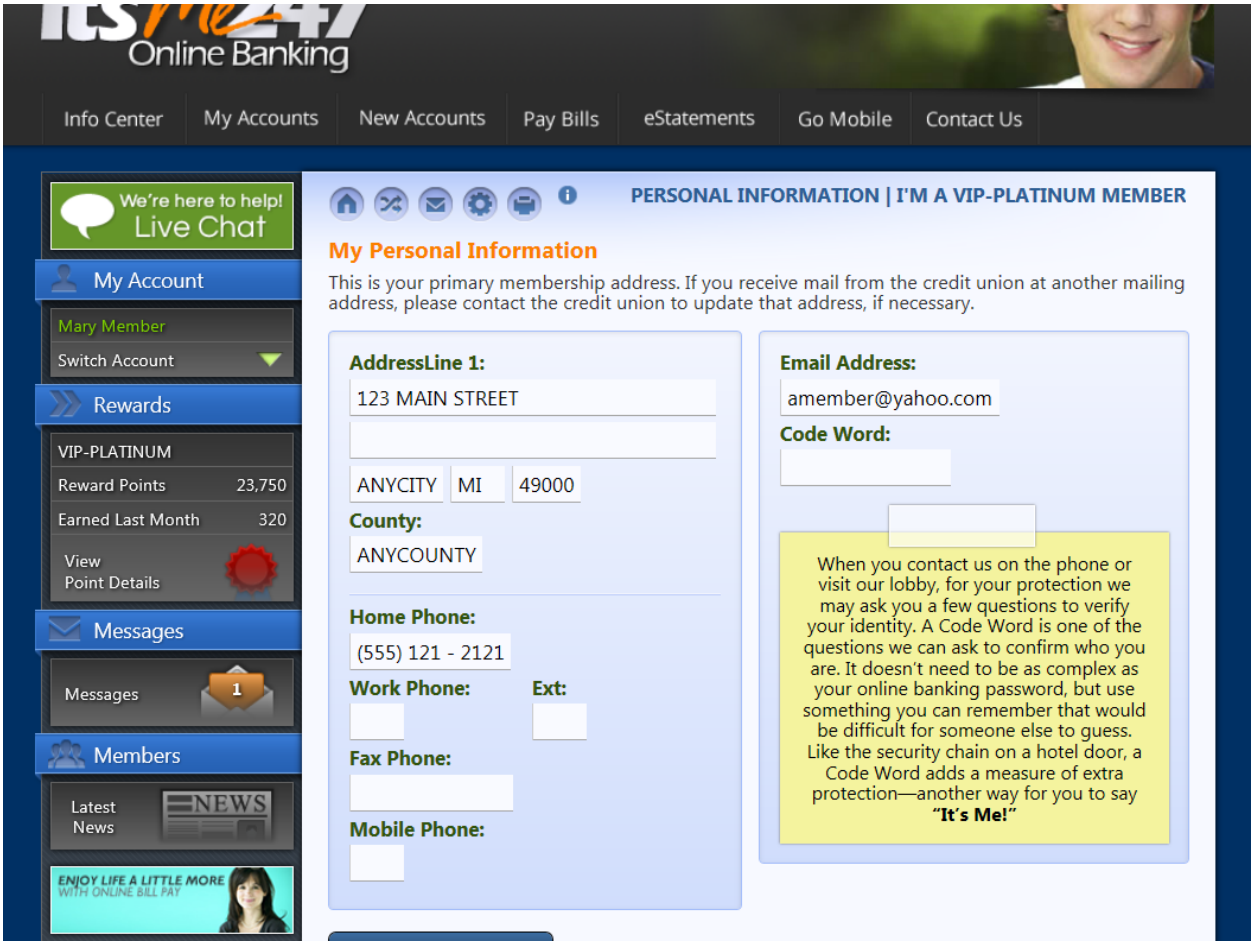
Members can by default update their personal information via the "My Information" page in online banking.

- NOTE: PIB allows you to block entry on the "My Information" page (shown on the following page) so it is not input capable. See Personal Internet Branch (PIB) Controls on page 14.

On the "My Information" page members can update the following items:

- Address Line 1
- Address Line 2
- City
- State
- Zipcode
- County
- Home Phone
- Work Phone
- Other Phone
- Fax Phone
- Email
- Code Word

My Information Page in It's Me 247



Members receive an email, and a message in the Secure Online Banking Message Center, any time a change is made to the "My Information" page in online banking. For email changes, the notification is sent to both the old and new email address.

- *NOTE: If the credit union is configured to review these changes prior to the system making the change, the email and message are sent when the approval is made.*
- Refer to the Communication with Members booklet (http://cuanswers.com/pdf/cb_ref/communication_with_members.pdf).

Personal Internet Branch (PIB) Controls

Credit union must first activate Personal Internet Branch (PIB). Contact a Client Services Representative for assistance.

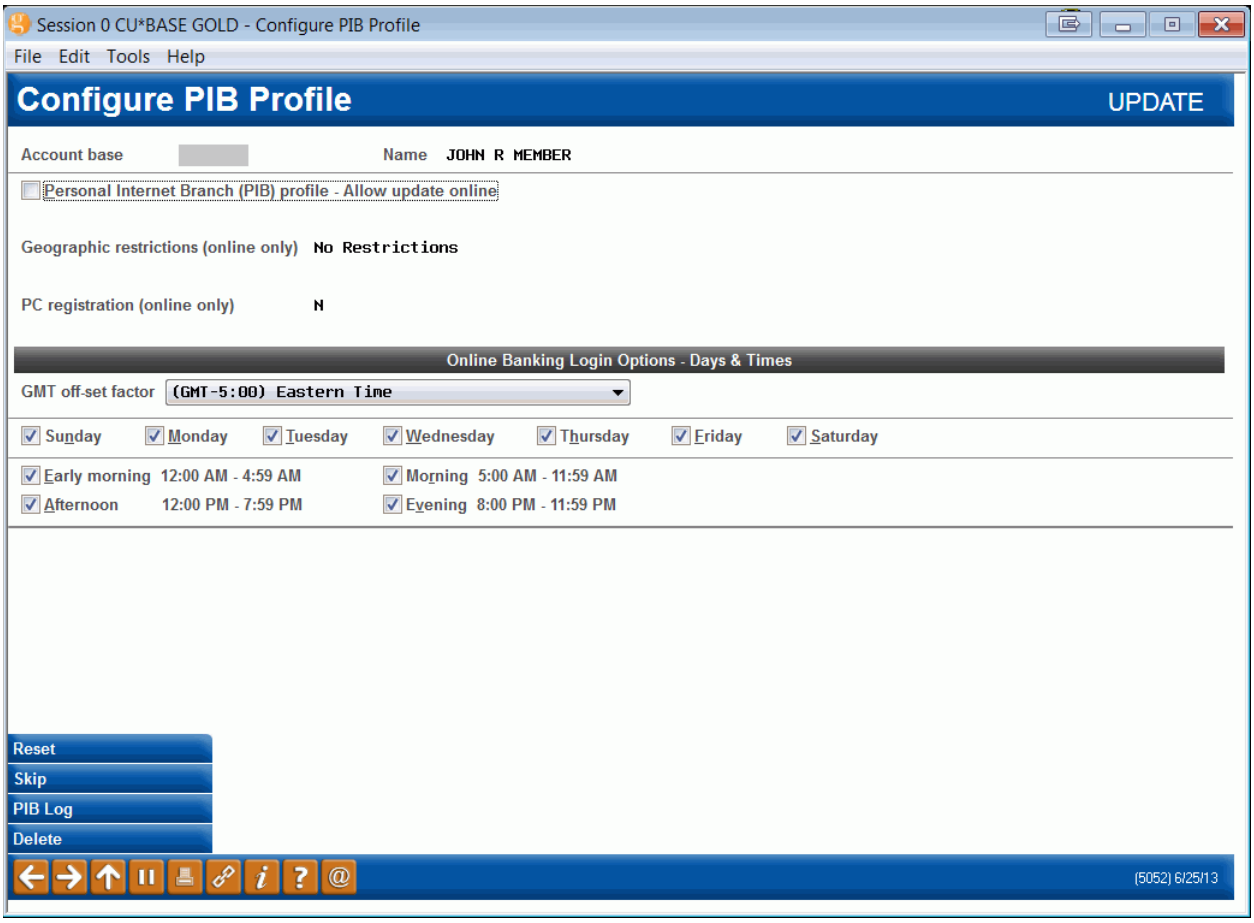
PIB is an independent application that provides multiple, configurable controls that govern how **It's Me 247** behaves and what members can do in online banking. It also provides member personalization, meaning that separate and unique controls can be set for each membership.

Through PIB, your credit union can determine which of the features you wish to allow in online banking. You can use the membership PIB screens to further define the permissions of each membership.

- Following are the Member Personal Banker PIB screens that are used to define PIB at a membership level. (Credit unions can also control PIB at the credit union level with other similar screens, which are accessed via **Tool #569** ***Online/Mobile/Text Banking VMS Config***.

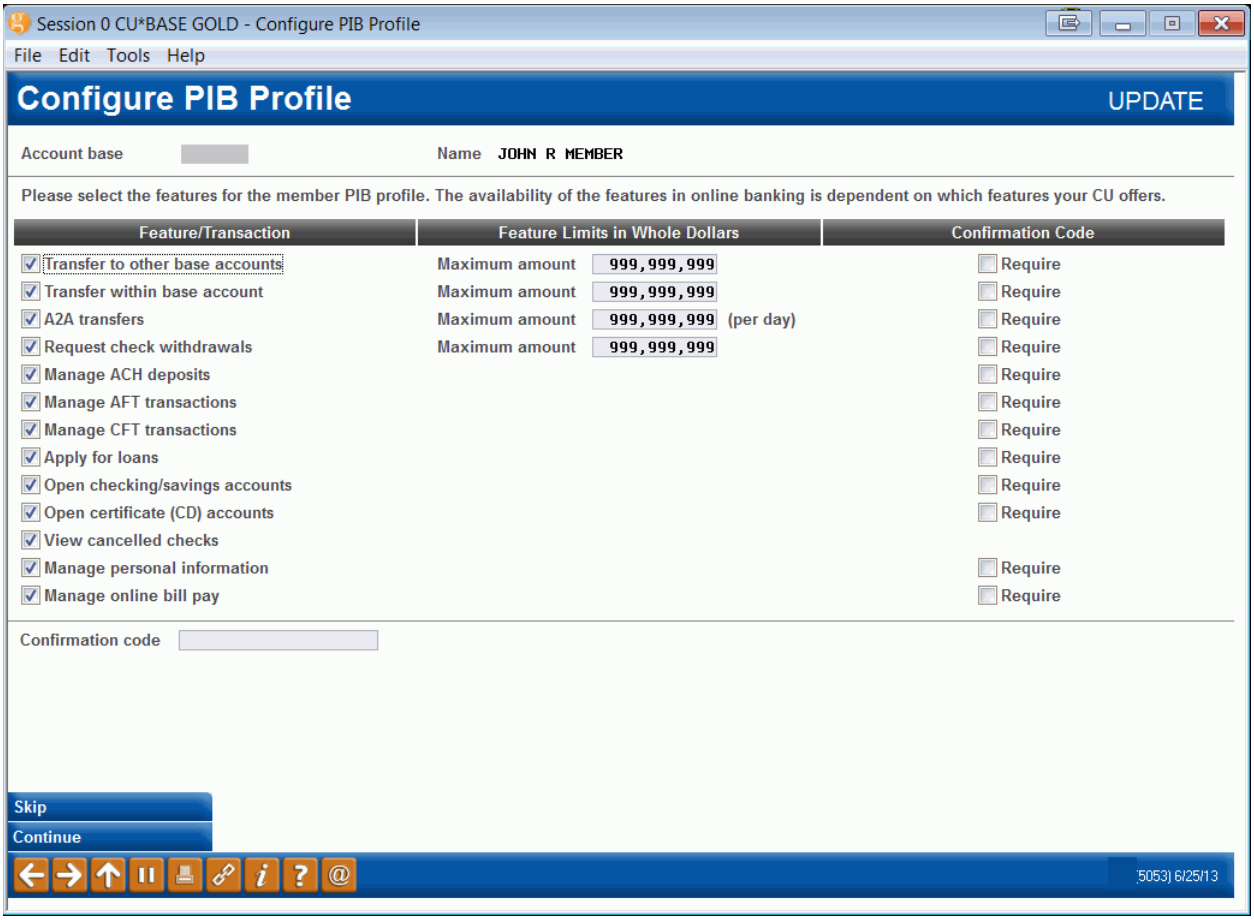
PIB can control the day of week and time of day a member can access his or her account:

PIB Configuration Screen (Days and Times)



PIB also controls whether a member can to the following:

PIB Configuration 2 (Transaction Activity and Other Controls)



- **Transfer to other accounts** - PIB also includes maximum amount per transfer controls
- **Transfers within base account** - PIB also includes maximum amount per transfer controls
- **A2A transfers** - PIB also includes maximum amount per day controls
- **Request check withdrawals** - issues a check that is sent to the member
- **Manage ACH Deposits**
- **Manage AFT transactions**
- **Manage CFT transactions** - sends a check to a name and address entered in online banking
- **Apply for loans**
- **Open checking/savings accounts**
- **Open certificate (CD) accounts**
- **View cancelled checks**
- **Manage personal information** - if this is unchecked a member cannot update the "My Information page (shown on page 13)
- **Pay bills online**

Using PIB, you can also require the entry of a confirmation code for all of the activities listed above, with the exception of "View Cancelled Checks." *NOTE: The confirmation code for "Pay Bills Online*

currently only applies to standard online banking, not Mobile Web Banking. Future enhancements are planned but not implemented at this time.

The member receives an email notification (as well as a message in the Secure Online Banking Message Center in online banking) any time a PIB setting or the confirmation code is changed.

IMPORTANT: If any change is made to the credit union controls of PIB, the credit union will also need to update its Default Profile, which serves as the basis for the member controls. Credit unions can update their Default PIB Profile via **Tool #378 *Flood PIB Default Profile Changes***. Refer to the CU*BASE Online help:

(http://help.cubase.org/cubase/#PPIBUPD-01.htm) or contact a Client Services Representative for assistance.

- Refer to the PIB: Configuration/User Guide (http://cuanswers.com/pdf/cb_ref/PIBConfigurationGuide.pdf)

Transfer Control Lists

Credit unions must first activate Transfer Control Lists. Contact a Client Services Representative for assistance.

A member's Transfer Control List determines to which memberships (at your credit union) the member can transfer funds. These memberships are presented to the member in Step 3 of the Transfer Wizard (Where is it going?) in standard online banking. Transfer Control lists also control to whom the member can transfer funds while in Mobile Web Banking.

This list affects other distributions of funds as well. Members are limited to the memberships on their Transfer Control List when creating either ACH Distributions or Automated Funds Transfers (AFTs) online.

Credit unions add memberships to a member's Transfer Control List via **Tool #883 *Update ARU/Online Banking Transfer Ctrl***. A member cannot add an account to his or her Transfer Control List while in online banking.