

## **Session 2**

# **FFIEC Guidance and Supplement to Authentication in an Internet Banking Environment**

Jim Vilker, NCCO

VP of Professional Services, CMS  
Audit Link, A Division of CU\*Answers

Patrick Sickels, JD, CISA, CRISC

Internal Auditor, CU\*Answers

Laura Welch-Vilker

Manager of Education Services, CU\*Answers

December 15, 2011

## *Agenda*

- Finalizing the risk assessment
- If necessary updating policies and procedures
- Updating the account opening process
  - CIP Cards and Procedures
- Utilizing It's Me 247 and PIB global settings
- Utilizing PIB individual settings
- Evaluating suspicious activity
- Member and staff educational requirements

## *Five Step Plan for FFIEC Compliance*

### ***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 (PIB)***

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***

Credit unions can already review the transactional history of clients for suspicious activity.

Furthermore, CU\*BASE is undergoing development to provide each credit union with more tools to monitor the transaction behavior of members. These new 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.

## *Risk Assessment Example*

### Overall Risk Assessment (Product Feature)

See sample:

<http://auditlink.cuanswers.com/2011/12/sample-its-me-247-risk-assessments-in-response-to-ffiec/>

*“Calling for all samples”*

# *Evaluating Results of Risk Assessment*

## **What will your risk assessment tell you?**

What if the credit union doesn't offer commercial accounts?

What if the credit union is SEG based and has very little suspicious activity?

What if the credit union has online commercial accounts?

What if the credit union already has suspicious activity?

*Based upon the answer to the above questions, the credit union will need to determine what changes are necessary to the:*

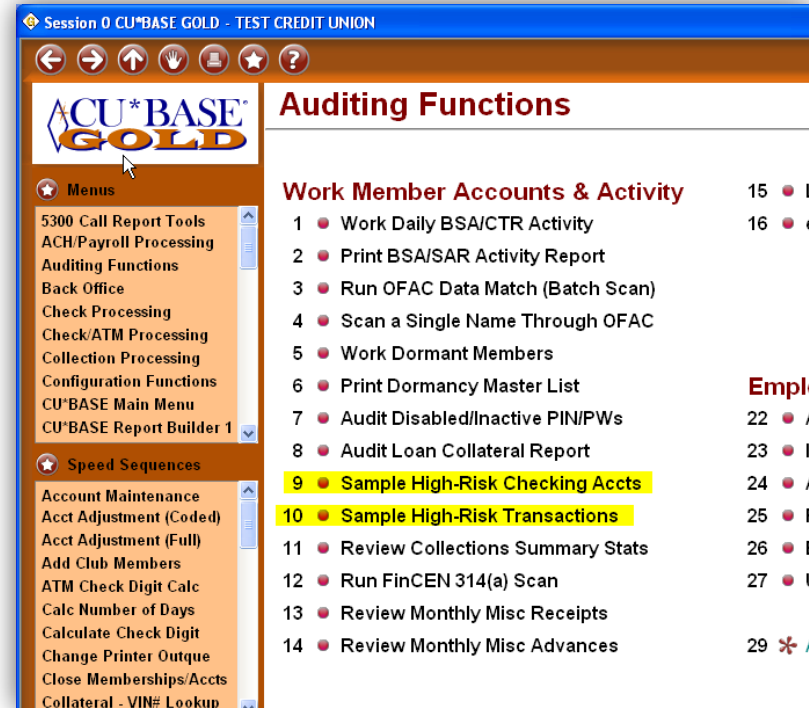
*Organization*

*Operations*

*Ongoing auditing and monitoring*

## Evaluating Suspicious Activity Using MNAUDT #9 and #10

All credit unions should perform this analysis when completing the risk assessment and based upon the findings of the assessment determine if this analysis needs to be preformed on a monthly basis for existing accounts.



## Tools for Completing Your Risk Assessment MNAUDT # 10

Session 6 CU\*BASE GOLD - Member Analysis

Member Analysis Nov 2011 Transaction Activity

Branch  00 = All branches  
Filter

Analysis Method	Sort
<a href="#">Go!</a> Teller Posting	D = Descending ▼
<a href="#">Go!</a> Loan Dept	D = Descending ▼
<a href="#">Go!</a> Share Drafts	D = Descending ▼
<a href="#">Go!</a> A T M	D = Descending ▼
<a href="#">Go!</a> Home Banking/A R U	D = Descending ▼
<a href="#">Go!</a> Online Credit Cards	D = Descending ▼
<a href="#">Go!</a> Debit Card	D = Descending ▼
<a href="#">Go!</a> A C H	D = Descending ▼
<a href="#">Go!</a> Phone Operator	D = Descending ▼
<a href="#">Go!</a> CU*EasyPay!	D = Descending ▼
<a href="#">Go!</a> Certificates	D = Descending ▼
<a href="#">Go!</a> Direct Mail Post	D = Descending ▼
<a href="#">Go!</a> Error Correction Processing	D = Descending ▼
<a href="#">Go!</a> Journal Transfers	D = Descending ▼
<a href="#">Go!</a> Social Security Deposits	D = Descending ▼

↑ ↓

Backup F3

Cancel F7

## *Ongoing Risk Assessment Maintenance*

1. Conduct on no less than an annual basis
2. Conduct whenever there is a major change to online banking offerings, account types, field of membership, merger, new cyber related threats
3. Provide education on no less than a yearly basis



## *Account Opening Procedures Changes to CIP card/process*

Questions to ask which trigger additional information gathering:

- Commercial in nature
- Expectation of high internet-based third party payments
- Classified by FFIEC as being high-risk
- Utilizing due diligence flag for high-risk accounts

## Example of Account Risk Assessment “Calling on all CIP cards”

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 <b>HIGH</b>
The transaction amounts are small	Small transactions to outside third parties, or larger transactions to parties within the credit union	Should be considered <b>MEDIUM</b>
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 <b>LOW</b>

# *Commercial 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.

# *Commercial Accounts*

<b>Control</b>	<b>Purpose</b>
<i>Email notification</i>	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
<i>Confirmation codes</i>	Requires a confirmation code before a high-risk transaction can be performed
<i>Password changes</i>	Should always be through the credit union, including changes to confirmation codes

## *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.

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.

*PIB should now be considered a **requirement** for any member engaging in high risk online banking activity. The credit union may wish to control PIB changes in-house, rather than have the member make these changes.*

## *Layered Security*

<b>Control</b>	<b>Purpose</b>
<i>Email notification</i>	<b>Should be used for every transaction that takes place in online banking</b> , as well as password resets and activation keys
<i>Transaction dollar limits</i>	<b>Critical in high risk transfers to outside third parties</b> ; configure the maximum dollars per day and per month
<i>Transaction time limits</i>	Restricts when transfers can take place; useful for businesses who do not need 24/7 online banking access
<i>Disable unused transactions</i>	Credit unions should disable all transactional activity not required by the consumer
<i>Set custom/complex PIN and passwords</i>	Should be recommended for any high risk transactions
<i>Audio banking</i>	Determines what activities are allowed over the phone
<i>PC Registration</i>	Restricts what PCs can be used to perform the transactions
<i>Geographic Location</i>	Restricts the locations where transactions can be performed
<i>Confirmation codes</i>	Requires a confirmation code before a high-risk transaction can be performed

## *Layered Security*

### **When?**

Ideally at account setup but  
ASAP for all high-risk accounts.

## Global Security Settings MNMGMC #16

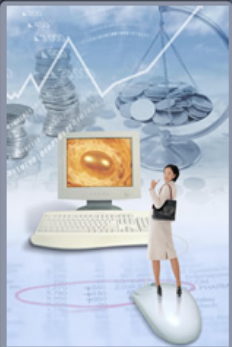
Session 6 CU\*BASE GOLD - ARU/Online Banking Configuration

←
→
↑
↓
⊞
★
?

Network Links

### ARU/Online Banking Configuration

UPDATE



Rates	F2
Update	F5
Cancel	F7
Connectivity	F11

Activation

Allow audio response     Activate audio response for new memberships

Allow online banking     Activate online banking for new memberships

PIN / Password Security Settings

# of password retries     Minimum length for online banking password (6 - 10)

Allow custom PIN/passwords    Expire password after  days of non-use (max = 90)

Enforce complex password online     Never expire (999)

Configure Online Banking Temporary Passwords

Set online banking temporary passwords to

Available Balance Calculation

Share - Deduct par value

CD - Deduct penalty

Deduct uncollected funds

Online Banking Use Agreement

Date   [MMDDYY]

Control Parameters

Transactions subject to Reg E     ACH distrib. maint. allowed     AET maint. allowed

Check requests allowed     CFT allow partial checks     CFT maint. allowed

Stop payments allowed     Inter-member transfers allowed

Retain stop pays  months/days     = Months

---

Check withdrawal minimum     Maximum     QFX download

Check image ID     Lag days

Check 21 processor



## MNCNFE #1

Session 6 CU\*BASE GOLD - Online Banking Configuration Options

Navigation icons: Back, Forward, Home, Stop, Refresh, Star, Help

Network Links

### Online Banking Configuration Options

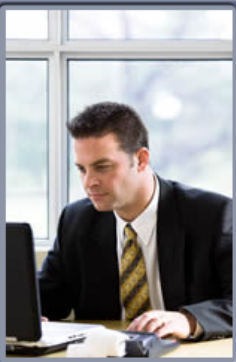
Corp ID 01

Configurable Options	
Standard Online Banking	
Mobile Banking	
e-Alerts/e-Notices	
Credit Union Email Address	
A2A Transfers	
PIB	
Default Photo Album	
Default Theme	
Default Start Page	
Helpful Links	

Cancel F7

Select

Up/Down arrows



## MNCNFE #1 – A2A

Session 6 CU\*BASE GOLD - Credit Union A2A Configuration

Network Links

### Credit Union A2A Configuration

Corp ID 01

	A2A Incoming	A2A Outgoing
Activate A2A transfers	<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Activate
Max \$ per day	100,000 (credit)	100,000 (debit)
Max \$ per last 30 days	500,000 (credit)	500,000 (debit)
Fee amount	0.00	0.00
Fee income G/L account	<input type="text"/>	<input type="text"/>


Clearing G/L account 706.15

Fee waivers:

Low age  High age 999 Aggregate savings 9,999,999.99 Aggregate loans 9,999,999.99

Waive if OTB account is present:  Credit  Loan  Savings  ATM  Debit

Allow fee to be manually waived



Backup F3

Update F5

Cancel F7

## MNCNFE #1 - PIB

Network Links

### Credit Union Default PIB Configuration

Corp ID 01

Personal Internet branch (PIB) profile - Allow update online

Online Banking Login Options - Days & Times Available

GMT off-set factor 5- = (GMT-5:00) Eastern Time

Session 6 CU\*BASE GOLD - Credit Union PIB Settings

Backup	F3
Cancel	F7
Cont to Default PIB Ent	

Corp ID 01

Activate personal Internet branch (PIB)

Require personal Internet branch (PIB) profile

Member can update transfer control list in PIB

BT (4239) [Learn About This Feature](#)

## MNCNFE #1 - PIB

Session 6 CU\*BASE GOLD - Credit Union Default PIB Configuration

Navigation icons: Back, Forward, Home, Stop, Refresh, Star, Help

Network Links

### Credit Union Default PIB Configuration

Corp ID 01

Personal Internet branch (PIB) profile - Allow update online

**Online Banking Login Options - Days & Times Available**

GMT off-set factor 5- = (GMT-5:00) Eastern Time

Sunday    Monday    Tuesday    Wednesday    Thursday    Friday    Saturday

Early morning 12:00 AM - 4:59 AM    Morning 5:00 AM - 11:59 AM

Afternoon 12:00 PM - 7:59 PM    Evening 8:00 PM - 11:59 PM

Backup	F3
Update	F5
Cancel	F7
Continue	Ent

## MNCNFE #1 - PIB

Session 6 CU\*BASE GOLD - Credit Union Default PIB Configuration

← → ↑ ↓ 🖨 ★ ?

Network Links

### Credit Union Default PIB Configuration

Backup	F3
Update	F5
Cancel	F7

Corp ID 01

Feature/Transaction	Feature Limits in Whole Dollar Amounts
<input checked="" type="checkbox"/> Transfer to other base accounts	Max amount <input type="text" value="100,000"/>
<input checked="" type="checkbox"/> Transfer within base account	Max amount <input type="text" value="100,000"/>
<input checked="" type="checkbox"/> Request check withdrawals	Max amount <input type="text" value="100,000"/>
<input checked="" type="checkbox"/> A2A transfers	Max amount <input type="text" value="100,000"/> (per day)
<input checked="" type="checkbox"/> Manage ACH deposits	
<input checked="" type="checkbox"/> Manage AFT transactions	
<input type="checkbox"/> Manage CFT transactions	
<input checked="" type="checkbox"/> Apply for loans	
<input checked="" type="checkbox"/> Open checking/savings accounts	
<input checked="" type="checkbox"/> Open certificate (CD) accounts	
<input checked="" type="checkbox"/> View cancelled checks	
<input checked="" type="checkbox"/> Manage personal information	
<input checked="" type="checkbox"/> Pay bills online	


Please select the features you wish to include in your default PIB profile.

## PIB at the Account Level - MNSERV # 22

Session 6 CU\*BASE GOLD - Member Personal Banker

← → ↑ ↓ ⌂ ☆ ? Network Links

### Member Personal Banker



Backup	F3
Cancel	F7
Bypass	F8

Account base	1000	Date opened	Oct 11, 2004
Name	TODD I FLINSTONE		
Agreement accepted	Jul 22, 2002		
E-Statements	000000	<input checked="" type="checkbox"/> PIB	
Bill payment	000000	<input type="checkbox"/> eAlerts/eNotices	

- E-statements (enroll or change enrollment status)
- Choose style for printed statements
- Bill Payment (enroll or change enrollment status)
- Bill Payment PIN reset
- Online banking/ARU (activate, change PIN/password; view password history)
- Online banking/ARU Transfer Control (update or add transfer accounts)
- Personal Internet Branch (enroll or change PIB settings)**
- PIB password reset (change PIB password or view PIB username)
- eAlerts/eNotices (subscribe or change settings; view eAlert history)
- A2A account relationships (add, modify, or remove relationships)
- Email address maintenance
- Reset online banking security questions
- Mobile banking (view member access and mobile devices)
- Debit card round up (enroll or change transfer account)
- Reg E opt in/out preference



## MNSERV #22 – Change PIB Settings

Session 6 CU\*BASE GOLD - Configure PIB Profile



Network Links

### Configure PIB Profile

UPDATE



Account base 1000

Name TODD I FLINSTONE

Personal Internet Branch (PIB) profile - allow update online

Geographic restrictions (online only) No restrictions

PC registration (online only)

#### Online Banking Login - Days and Times Available

Timezone 5- = GMT -5:00 Eastern Time

Sunday

Early Morning 12:00 AM - 4:59 AM

Monday

Morning 5:00 AM - 11:59 AM

Tuesday

Afternoon 12:00 PM - 7:59 PM

Wednesday

Evening 8:00 PM - 11:59 PM

Thursday

Friday

Saturday

Backup	F3
Reset	F6
Cancel	F7
Bypass	F8
PIB Log	F10
Delete	F16
Continue	Ent

## MNSERV #22 – Change PIB Settings

Session 6 CU\*BASE GOLD - Configure PIB Profile

⏪ ⏩ ⌂

⏪
⏩
⏴
⏵
⏶
⏷
⏸


Network Links

---

### Configure PIB Profile

UPDATE

---



Backup	F3
Cancel	F7
Bypass	F8
Continue	Ent

Account base **1000** Name **TODD I FLINSTONE**

---

Please select the features for the member PIB profile. The availability of the features in online banking is dependent on which features your credit union offers.

Feature/Transaction	Feature Limits in Whole Dollar Amounts	Confirmation Code
<input checked="" type="checkbox"/> Transfer to other base accounts	Maximum amount <b>999,999,999</b>	<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Transfer within base account	Maximum amount <b>999,999,999</b>	<input type="checkbox"/> Require
<input type="checkbox"/> A2A transfers	Maximum amount <b>999,999,999</b> (per day)	<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Request check withdrawals	Maximum amount <b>999,999,999</b>	<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Manage ACH deposits		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Manage AFT transactions		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Manage CFT transactions		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Apply for loans		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Open checking/savings accounts		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Open certificate (CD) accounts		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> View cancelled checks		
<input checked="" type="checkbox"/> Manage personal information		<input type="checkbox"/> Require
<input checked="" type="checkbox"/> Manage online bill pay		<input checked="" type="checkbox"/> Require

---

Confirmation code



*PIB Member Experience*

## Ongoing Monitoring – MNAUDT # 10

Session 6 CU\*BASE GOLD - Member Analysis

Member Analysis Nov 2011 Transaction Activity

Branch  00 = All branches  
 Filter

Analysis Method	Sort
<a href="#">Go!</a> Teller Posting	D = Descending
<a href="#">Go!</a> Loan Dept	D = Descending
<a href="#">Go!</a> Share Drafts	D = Descending
<a href="#">Go!</a> A T M	D = Descending
<a href="#">Go!</a> Home Banking/A R U	D = Descending
<a href="#">Go!</a> Online Credit Cards	D = Descending
<a href="#">Go!</a> Debit Card	D = Descending
<a href="#">Go!</a> A C H	D = Descending
<a href="#">Go!</a> Phone Operator	D = Descending
<a href="#">Go!</a> CU*EasyPay!	D = Descending
<a href="#">Go!</a> Certificates	D = Descending
<a href="#">Go!</a> Direct Mail Post	D = Descending
<a href="#">Go!</a> Error Correction Processing	D = Descending
<a href="#">Go!</a> Journal Transfers	D = Descending
<a href="#">Go!</a> Social Security Deposits	D = Descending

Backup F3  
Cancel F7

↑ ↓

## *Member Education*

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.

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.*

## *Member Education*

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

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.

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

## *Sharing Information*

CU\* Answers ExamShare and PolicySwap will be live March 1, 2012. Until that time, please share your:

Assessments

Policies

CIP cards and procedures

## *What's Next*

- Mid January web conference for reviewing examination checklist (if completed by FFIEC) and peer processes and policies (collaborative with CU\*Answers clients)

## *Reference Material*

PIB Made Simple – Try it with your staff

[http://cuanswers.com/pdf/cb\\_ref/PIBStaffTryIt.pdf#2009-02-12](http://cuanswers.com/pdf/cb_ref/PIBStaffTryIt.pdf#2009-02-12)

Roll-Out Strategies

[http://cuanswers.com/pdf/cb\\_ref/PIBRollout.pdf#2010-10-12](http://cuanswers.com/pdf/cb_ref/PIBRollout.pdf#2010-10-12)

PIB Configuration and User Guide

[http://cuanswers.com/pdf/cb\\_ref/PIBConfiguration.pdf#2011-12-09](http://cuanswers.com/pdf/cb_ref/PIBConfiguration.pdf#2011-12-09)

Answering Your Questions about PIB

<http://cuanswers.com/pdf/security/CUFAQs.pdf#2007-12-07>

# *Questions?*





## *LEGAL DISCLAIMER*

The information contained in this email does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this email. 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.