October 4, 2011

Your Guide to Compliance:
FFIEC Supplement to Authentication in an Internet Banking Environment

Contents

LEGAL DISCLAIMER

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

Introduction

The Federal Financial Institution Examination Council, or FFIEC, in 2011 issued the *Supplement to Authentication in an Internet Banking Environment*. This document includes new "Specific Supervisory Expectations" for all financial institutions with respect to online banking. The NCUA has declared that all credit unions are subject to examination based on the *Supplement* starting in 2012. For credit unions this means increased supervisory and legal risks associated with online banking.

However, our Network credit unions should be aware that this risk can be mitigated effectively by utilizing the tools with CU*BASE. In fact, following this *Compliance Guide*, a credit union can not only expect to pass supervisory examinations but will vastly reduce the security and liability risks associated with online banking. CU*BASE offers every credit union that processes online financial transactions the power to safeguard member assets and move towards compliance with the new regulatory requirements.

Supplement Essentials

In many ways, the *Supplement* does not break substantial new ground regarding online banking security. Rather, the FFIEC is recognizing the fact that there has been an increase in fraudulent activity in online banking that reflects the growing prevalence of online banking throughout the financial services industry. As greater amounts of funds continued to be transferred online, relying on authentication alone for transaction verification entails significant risk for both the member and the credit union. Member online banking credentials can be compromised through many means, exposing the member and the credit union to risk of loss.

In addition to requiring risky online accounts to have more security than just authentication, the FFIEC also expects financial institutions to avoid processing suspicious electronic transactions. Even if the consumer is partially negligent by using their account insecurely, the financial institution can still be held liable if the transactions processed were suspicious.

Unfortunately, the FFIEC failed to define "suspicious or anomalous activity" in the *Supplement*. But it would appear to require a significant deviation from normal member behavior to trigger liability for the credit union. Furthermore, our opinion is that credit unions are better off by focusing efforts on strengthening their layered security controls than relying heavily on suspicious transaction detection.

A Five-Step Plan for *Supplement* Compliance

This five step plan will help credit unions successfully comply with the new Supervisory Expectations in the *Supplement*:

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
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.

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

The FFIEC definition of high risk transactions remains electronic transactions involving access to customer information or the movement of funds to other parties. Thus, 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 stolen funds can be 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 MNAUDT #10 – Sample High-Risk Transactions CCD to analyze the riskiness of the accounts. In addition, credit unions can use Due Diligence (DD) 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.

CU*Answers offers two documents for helping credit unions complete online banking risk assessments. Completing your Credit Union's Internet Banking Risk Assessment is a how to guide on writing your online banking risk assessment. The It's Me 247 Online Banking Risk Assessment: Product Feature Matrix contains details on the **It's Me 247** security features available to your credit union and members.

Step Two: If Commercial or Deemed to be High Risk at Account Opening, Set Administrative Functions

The FFIEC wants financial institutions to take additional care when it comes to commercial online banking accounts and those accounts which you deem to be high risk by virtue of the questions answered at account opening. Credit unions need to ensure that these 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.

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 in PIB for commercial online banking accounts include:

Control	Purpose
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
Confirmation codes	Requires a confirmation code before a high-risk transaction can be performed
Password changes	Should always be through the credit union, including changes to confirmation codes

The PIB Configuration Manual provides details on how to configure PIB settings for your members.

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 allowing transactions from only certain computers and limits 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.

*Note: 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.*

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

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

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.

The PIB Configuration Manual provides details on how to configure PIB settings for your members.

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.

The easiest way to uncover suspicious activity is through the use the suspicious activity monitoring features found in MNAUDT options #9 and #10. These options analyze the total activity a member has had for a given month by transaction origin and list from high to low the total transaction counts. The credit union should pay particular attention to those origins specifically related to internet banking such as log-ons, account to external account transfer, member transfers to other internal accounts, and ACH activity, as this could be the result of bill pay.

To further meet this requirement, CU*Answers is developing additional toolsets within CU*BASE to allow credit unions to analyze the transaction behavior of members and flag activities that are anomalous or suspicious for any period of time the credit union desires. 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 early 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.