How the updated FFIEC guidance on Internet banking security affects your credit union

Prepared by:

Chris Fisher, *Director*, McGladrey LLP
805.404.9455, chris.fisher@mcgladrey.com

October 2012

On June 28, 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a supplement (the Supplement) to the Authentication in an Internet Banking Environment (the 2005 Guidance). National Credit Union Administration examiners began monitoring the new guidance standards beginning in January 2012. The purpose of the Supplement is to reinforce the risk management framework described in the original guidance and to update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security and other controls in the increasingly volatile online environment. The agencies were concerned that customer authentication methods and controls implemented in conformance with the 2005 Guidance had become less effective.

The FFIEC which includes the board of governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency and Office of Thrift Supervision, released the 2005 Guidance on Oct. 12, 2005. The 2005 Guidance provided a risk management framework for financial institutions that offer Internet-based products and services to their members. It stated that institutions should use effective methods to authenticate the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered, and sufficient to protect sensitive customer information. The 2005 Guidance provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties. The 2005 Guidance also provided that institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing and external threats.

The Supplement stresses the need for performing risk assessments, implementing effective strategies for mitigating identified risks and raising member awareness of potential risks, but does not endorse any specific technology for doing so. The Supplement's primary focus is on preventing attacks by rootkit-based malware, conducting stronger risk assessments and implementing layered security controls. The FFIEC member agencies have directed examiners to formally assess financial institutions under the enhanced expectations outlined in the Supplement from January 2012 onwards. Examiners are charged with ensuring that a process is in place to detect and respond to suspicious activity at initial login to an electronic banking system and at the initiation of electronic transactions involving funds transfers.

The Supplement establishes specific supervisory expectations in three areas – risk assessments, layered security controls, and member awareness and education.

Risk assessments

FFIEC reinforced the expectations that credit unions should perform periodic risk assessments and adjust their member authentication controls as appropriate in response to new threats to members' online accounts. To ensure compliance with the guidelines, credit unions cannot rely solely on any single control for authorizing high-risk transactions. Instead, they should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every 12 months. Updated risk assessments should consider, but not be limited to, the following factors:

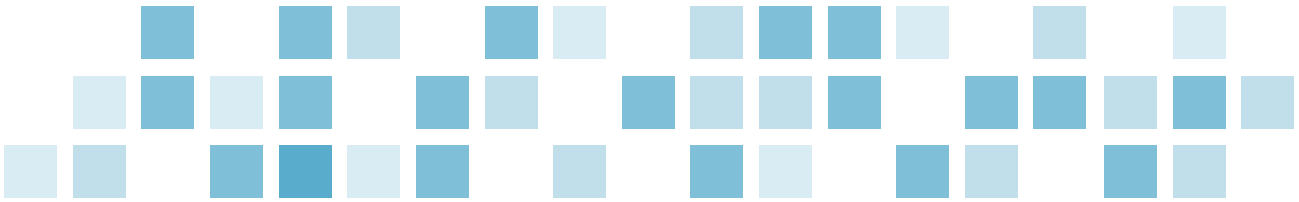
- Changes in the internal and external threat environment
- Changes in the how the member base is adopting electronic banking
- Changes in the functionality offered to members through electronic banking
- Actual incidents of security breaches, identity theft or fraud experienced by the institution or industry

Layered security controls

The updated guidance recognizes that the risks posed to retail and consumer banking are lower than the risks currently posed to business and commercial banking. However, layered security is required for both.

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Layered security can substantially strengthen the overall security of Internet-based services. Layered security can be effective in protecting sensitive member information, preventing identity theft, and in reducing account takeovers and the resulting financial losses. Effective controls that may be included in a layered security program include, but are not limited to:

- Fraud detection and monitoring systems that consider member history and behavior and enable a timely and effective institution response
- The use of dual member authorization through different access devices
- The use of out-of-band verification for transactions
- The use of positive pay debit blocks and other techniques to appropriately limit the transactional use of the account
- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, a limit to the number of transactions allowed per day and allowable payment windows
- Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities
- Policies and practices for addressing member devices identified as potentially compromised and for dealing with members who may be facilitating fraud
- Enhanced control over changes to account maintenance activities performed by members either online or through member service channels
- Enhanced member education to increase awareness of the fraud risk and effective techniques members can use to mitigate the risk



Layered security is expected to address the following two elements, at a minimum:

- Improve the ability of the security for online accounts to detect and respond to suspicious activity at the initial login and during the initiation of any electronic funds transfers
- Enhance the security controls for administrative privileges to user setup, application configurations and limitations

Each additional measure materially increases the level of difficulty for an attacker.

Member awareness and education

A credit union's member awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- 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 circumstances under which, and the means by which, the credit union may contact a member on an unsolicited basis in order to request the member's electronic banking credentials
- A suggestion that commercial online banking members perform a related risk assessment and controls evaluation periodically
- A listing of alternative risk control mechanisms that members may consider implementing in order to mitigate their own risk; or, alternatively, a listing of available resources where such information can be found
- A listing of institutional contacts for members' discretionary use in the event they notice suspicious account activity or experience security-related information events

An overview of threats and compensating controls is presented in the appendix to the Supplement. Key points identified in the appendix include keyloggers and man-in-the middle (MIM) or man-in-the-browser (MIB) attacks, which are highlighted as threats. MIB attacks are being used to circumvent strong authentication methods, such as one-time password (OTP) tokens.

The appendix indicates that out-of-band authentication or verification has taken on an increased level of importance given the rising malware infection rates on member PCs, which can defeat OTP tokens, device identification, challenge questions and many other forms of strong authentication.

Discussion also includes a look forward to emerging security controls, such as keystroke dynamics, biometrics, volume and value limitations, monitoring and alert on exception events, establishing individual transaction and aggregate account exposure limits based on expected account activity, and dual controls over high-risk functions performed online.

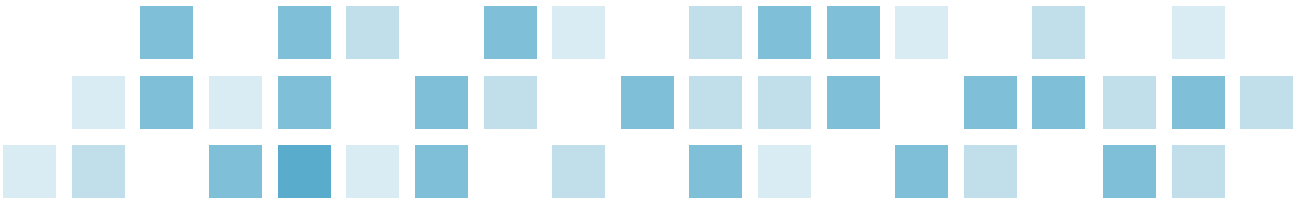
Preparing for the 2012 regulatory examination

According to Guardian Analytics, a provider of behavioral analytics-based fraud prevention solutions, just more than half of the financial institutions it surveyed are ready for the FFIEC guidance. Of the 300 U.S. institutions surveyed, 75 percent of banks and 25 percent of credit unions say they have spent the last six months on conformance action; however, only 50 percent say they fully understand minimum requirements for authentication conformance.

National Credit Union Administration examiners have been monitoring the new guidance standards since January 2012. Examiners expect credit unions have a process in place to continuously monitor and updatetheir compliance and risk management practices to adjust for new information and changes in the business, compliance and risk landscape. Credit unions should act now, if they haven't already, to complete the necessary steps to achieve compliance. These include the following:

- Review and update your IT risk assessment and consider new information that is detailed in the Supplement
- Work with your managed service provider, core provider or other online banking solution provider to begin evaluating stronger authentication techniques such as basic challenge questions or simple device identification that can supplement weaker methods.
- Consider whether you need to add additional controls throughout your security program, including those on high-risk transactions, remote employee access to customer data and business accounts
- Enhance customer awareness programs and educational programs

The Supplement is just the first step in the process. Many in the security industry expect to see additional refinements in the future. The Supplement provides a solid baseline for authentication and security efforts and creates a need for credit unions to take a stronger look at fraud and security. Making security a key element for all strategic plans protects both your members and your reputation from avoidable risks. Preparation is the key. Credit unions can never be too prepared when it comes to protecting their members.



800.274.3978
www.mcgladrey.com

McGladrey LLP is the U.S. member of the RSM International ("RSMI") network of independent accounting, tax and consulting firms. The member firms of RSMI collaborate to provide services to global clients, but are separate and distinct legal entities which cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party.

McGladrey, the McGladrey signature, The McGladrey Classic logo, *The Power of Being Understood*, *Power Comes from Being Understood* and *Experience the Power of Being Understood* are trademarks of McGladrey LLP.

© October 2012 McGladrey LLP. All Rights Reserved.