Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-50-2011
June 29, 2011

FFIEC Supplement to *Authentication in an Internet Banking Environment*

Summary: The FDIC, with the other FFIEC agencies, has issued the attached guidance, which describes updated supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment. Financial institutions will be expected to comply with the guidance no later than January 1, 2012.

Statement of Applicability to Institutions with Total Assets under $1 billion: This Financial Institution Letter applies to all FDIC-supervised institutions offering online banking services**.**

Suggested Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:

- FIL-103-2005, Authentication in an Internet Banking Environment, October 12, 2005

Attachment:
FFIEC Supplement to Authentication in an Internet Banking Environment

Contact:
Jeffrey Kopchik, Senior Policy Analyst, at jkopchik@fdic.gov or (202) 898-3872

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2010/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- In 2005, the FFIEC issued guidance entitled *Authentication in an Internet Banking Environment*.
- This FFIEC guidance supplements the FDIC's supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment.
- The FDIC expects institutions to upgrade their controls for high-risk online transactions through:
  - Yearly risk assessments;
  - For consumer accounts, layered security controls;
  - For business accounts, layered security controls consistent with the increased level of risk posed by business accounts; and
  - More active consumer awareness and education efforts.
- Layered security controls should include processes to detect and respond to suspicious or anomalous activity and, for business accounts, administrative controls.
- Certain types of device identification and challenge questions should no longer be considered effective controls.

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 •
http://www.ffiec.gov

Supplement to
Authentication in an Internet Banking Environment

Purpose

On October 12, 2005, the FFIEC agencies[1] (Agencies) issued guidance entitled *Authentication in an Internet Banking Environment* (2005 Guidance or Guidance).[2] The 2005 Guidance provided a risk management framework for financial institutions offering Internet-based products and services to their customers. 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 the protection of sensitive customer information. The 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 internal and external threats.

The purpose of this Supplement to the 2005 Guidance (Supplement) is to reinforce the Guidance's risk management framework and update the Agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment. The Supplement reiterates and reinforces the expectations described in the 2005 Guidance that financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security, and other controls as appropriate in response to identified risks. It establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment. It also

[1] 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.
[2] FRS SR Letter 05-19, October 13, 2005; FDIC Financial Institution Letter 103-2005, October 12, 2005; NCUA Letter to Credit Unions 05-CU-18, November 2005; OCC Bulletin 2005-35, October 2005; OTS CEO Memorandum 228, October 12, 2005.

identifies certain specific minimum elements that should be part of an institution's customer awareness and education program.

Background

Since 2005, there have been significant changes in the threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and permitting their use by less experienced fraudsters. Rootkit-based malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication. Cyber crime complaints have risen substantially each year since 2005, particularly with respect to commercial accounts. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.[3]

The Agencies are concerned that customer authentication methods and controls implemented in conformance with the Guidance several years ago have become less effective. Hence, the institution and its customers may face significant risk where periodic risk assessments and appropriate control enhancements have not routinely occurred.

General Supervisory Expectations

The concept of customer authentication, as described in the 2005 Guidance, is broad. It includes more than the initial authentication of the customer when he/she connects to the financial institution at login. Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security, as described herein.

[3] See IC3 Annual Internet Crime Reports 2005-2009.

Specific Supervisory Expectations

Risk Assessments

The Agencies reiterate and stress the expectation described in the 2005 Guidance that financial institutions should perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts. Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months.[4] Updated risk assessments should consider, but not be limited to, the following factors:

- changes in the internal and external threat environment, including those discussed in the Appendix to this Supplement;
- changes in the customer base adopting electronic banking;
- changes in the customer functionality offered through electronic banking; and
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

Customer Authentication for High-Risk Transactions

The 2005 Guidance's definition of "high-risk transactions" remains unchanged, i.e., electronic transactions involving access to customer information or the movement of funds to other parties. However, since 2005, more customers (both consumers and businesses) are conducting online transactions. The Agencies believe that it is prudent to recognize and address the fact that not every online transaction poses the same level of risk. Therefore, financial institutions should implement more robust controls as the risk level of the transaction increases.

Retail/Consumer Banking

Online consumer transactions generally involve accessing account information, bill payment, intrabank funds transfers, and occasional interbank funds transfers or wire transfers. Since the frequency and dollar amounts of these transactions are generally lower than commercial transactions, they pose a comparatively lower level of risk. Financial institutions should implement layered security, as described herein, consistent with the risk for covered consumer transactions.

---

[4] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Risk Assessment Practices section.

Business/Commercial Banking

Online business transactions generally involve ACH file origination and frequent interbank wire transfers. Since the frequency and dollar amounts of these transactions are generally higher than consumer transactions, they pose a comparatively increased level of risk to the institution and its customer. Financial institutions should implement layered security, as described herein, utilizing controls consistent with the increased level of risk for covered business transactions. Additionally, the Agencies recommend that institutions offer multifactor authentication to their business customers.

Layered Security Programs

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 and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses. It should be noted that other regulations and guidelines also specifically address financial institutions' responsibilities to protect customer information and prevent identity theft.[5] Financial institutions should implement a layered approach to security for high-risk Internet-based systems.[6]

Effective controls that may be included in a layered security program include, but are not limited to:

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer 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, number of transactions allowed per day, and allowable payment windows (e.g., days and times);

---

[5] See Interagency Final Regulation and Guidelines on Identity Theft Red Flags, 12 CFR parts 41, 222, 334, 571, and 717; Interagency Guidelines Establishing Information Security Standards, 12 CFR parts 30, 208, 225, 364, and 570, Appendix B.

[6] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Concepts section.

- 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 customer devices identified as potentially compromised and customers who may be facilitating fraud;
- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

The Agencies expect that an institution's layered security program will contain the following two elements, at a minimum.

Detect and Respond to Suspicious Activity

Layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

- initial login and authentication of customers requesting access to the institution's electronic banking system; and
- initiation of electronic transactions involving the transfer of funds to other parties.

Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior.

Control of Administrative Functions

For business accounts, layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. These enhanced controls should exceed the controls applicable to routine business customer users. For example, a preventive control could include requiring an additional authentication routine or a transaction verification routine prior to final implementation of the access or application changes. An example of a detective control could include a transaction verification notice immediately following implementation of the submitted access or application changes. As discussed in the Appendix, out-of-band

authentication, verification, or alerting can be effective controls. Based upon the incidents the Agencies have reviewed, enhanced controls over administrative access and functions can effectively reduce money transfer fraud.

Effectiveness of Certain Authentication Techniques

Device Identification

In response to the 2005 Guidance, many financial institutions implemented simple device identification. This typically uses a cookie loaded on the customer's PC to confirm that it is the same PC that was enrolled by the customer and matches the logon ID and password that is being provided. However, experience has shown this type of cookie may be copied and moved to a fraudster's PC, allowing the fraudster to impersonate the legitimate customer. Device identification has also been implemented using geo-location or Internet protocol address matching. However, increasing evidence has shown that fraudsters often use proxies, which allow them to hide their actual location and pretend to be the legitimate user.[7]

Simple device identification as described above can be distinguished from a more sophisticated form of this technique which uses "one-time" cookies and creates a more complex digital "fingerprint" by looking at a number of characteristics including PC configuration, Internet protocol address, geo-location, and other factors.[8] Although no device authentication method can mitigate all threats, the Agencies consider complex device identification to be more secure and preferable to simple device identification. Institutions should no longer consider simple device identification, as a primary control, to be an effective risk mitigation technique.

Challenge Questions

Many institutions use challenge questions as a backup in the event that the primary logon authentication technique becomes inoperable or presents an unexpected characteristic. The provision of correct responses to challenge questions can also be used to re-authenticate the customer or verify a specific transaction subsequent to the initial logon. Similar to device identification, challenge questions can be implemented in a variety of ways that impact their effectiveness as an authentication tool. In its basic form, the user is presented with one or more simple questions from a list that was first presented to the

[7] The National Security Agency has developed a patented method, available for public licensing, that can detect the use of a proxy.

[8] Technology vendors have developed "one-time" cookies which expire if stolen from the PC onto which they were originally loaded.

customer when they originally enrolled in the online banking system. These questions can often be easily answered by an impostor who knows the customer or has used an Internet search engine to get information about the customer (e.g., mother's maiden name, high school the customer graduated from, year of graduation from college, etc.). In view of the amount of information about people that is readily available on the Internet and the information that individuals themselves make available on social networking websites, institutions should no longer consider such basic challenge questions, as a primary control, to be an effective risk mitigation technique.

Challenge questions can be implemented more effectively using sophisticated questions. These are commonly referred to as "out of wallet" questions, that do not rely on information that is often publicly available. They are much more difficult for an impostor to answer correctly. Sophisticated challenge question systems usually require that the customer correctly answer more than one question and often include a "red herring" question that is designed to trick the fraudster, but which the legitimate customer will recognize as nonsensical. The Agencies have also found that the number of challenge questions employed has a significant impact on the effectiveness of this control. Solutions that use multiple challenge questions, without exposing all the questions in one session, are more effective. Although no challenge question method can mitigate all threats, the Agencies believe the use of sophisticated questions as described above can be an effective component of a layered security program.

Customer Awareness and Education

A financial institution's customer 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 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;
- 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; and,

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

The attached Appendix contains an additional discussion of online threats and control methods.

Appendix

Threat Landscape and Compensating Controls

Threats

As noted previously in this Supplement, the Agencies are concerned that fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of customer accounts, and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement. Many of these schemes target small to medium-sized business customers since their account balances are generally higher than consumer accounts and their transaction activity is generally greater making it easier to hide the fraudulent transfers.

An effective tool in the fraudster's arsenal is keylogging malware. A keylogger is a software program that records the keystrokes entered on the PC on which it is installed and transmits a record of those keystrokes to the person controlling the malware over the Internet. Keyloggers can be surreptitiously installed on a PC by simply visiting an infected website or by clicking on an infected website banner advertisement or email attachment. Keylogging can also be accomplished via a hardware device plugged into the PC which stores the captured data for later use. Keylogger files are generally small in size and adept at hiding themselves on the user's PC. They often go undetected by most antivirus programs. Fraudsters use keyloggers to steal the logon ID, password, and challenge question answers of financial institution customers. This information alone or in conjunction with stolen browser cookies loaded on the fraudster's PC may enable the fraudster to log into the customer's account and transfer funds to accounts controlled by the fraudster, usually through wire or ACH transactions.

Other types of more sophisticated malware allow fraudsters to perpetrate man-in-the middle (MIM) or man-in-the browser (MIB) attacks on their victims. In a MIM/MIB attack, the fraudster inserts himself between the customer and the financial institution and hijacks the online session. In one scenario, the fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account. In another scenario, the fraudster does not intercept the credentials, but modifies the transaction content or inserts additional transactions not authorized by the customer which, in most cases, are funds transfers to accounts controlled by the fraudster. The fraudsters conceal

their actions by directing the customer to a fraudulent website that is a mirror image of the financial institution's website or sending the customer a message claiming that the institution's website is unavailable and to try again later. Fraudsters may have the capacity to delete any trace of their attack from the log files.

MIM/MIB attacks may be used to circumvent some strong authentication methods and other controls, including one-time password (OTP) tokens. OTP tokens have been used for several years and have been considered to be one of the stronger authentication technologies in use. Since the one-time password is generally only good for 30-60 seconds after it is generated, the fraudster must intercept and use it in real time in order to compromise the customer's account.

Controls

The Agencies are aware of a variety of security techniques which can be used to help detect and prevent the types of attacks described above. Some of these techniques have been in use for some time, while others are relatively new. Financial institutions should investigate which of these controls may be more effective in detecting and preventing attacks as part of the institution's layered security program. However, it is important to note, that none of the controls discussed provide absolute assurance in preventing or detecting a successful attack. These controls may include the following:

Anti-malware software may provide a defense against keyloggers and MIM/MIB attacks. Anti-malware is a term that is commonly used to describe various software products that may also be referred to as anti-virus or anti-spyware. Anti-malware software is used to prevent, detect, block, and remove adware, spyware, and other forms of malware such as keyloggers. It is important to note that anti-malware is generally signature based, and some advanced versions of malware continuously alter their signature.

Transaction monitoring/anomaly detection software has been in use for a number of years. Similar to the manner in which the credit card industry detects and blocks fraudulent credit card transactions, systems are now available to monitor online banking activity for suspicious funds transfers. They can stop a suspicious ACH/wire transfer before completion and alert the institution and/or the customer so that the transfer can be further authenticated or dropped. Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring/anomaly detection could have assisted in preventing many fraudulent money transfers as they were clearly out of the ordinary when compared with the customer's established patterns of behavior. Automated

systems may also look at the velocity of a transaction and other similar factors to determine whether it is suspicious.

The Agencies are aware of the fact that a number of institutions are requiring the "out-of-band" authentication or verification of certain high value and/or anomalous transactions. Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised. For business customers, the out-of-band authentication or verification can be provided by someone other than the person who first initiated the transaction and can be combined with other administrative controls. Additionally, the use of out-of-band authentication or verification, for administrative changes to online business accounts, can be an effective control to reduce fraudulent funds transfers.

In response to the rising malware infection rates of customer PCs, a number of vendors have developed USB devices that increase session security when plugged into the customer's PC. These devices can function in several ways, but they generally enable a secure link between the customer's PC and the financial institution independent of the PC's operating system and application software. Typically, the device's firmware is "read only" and cannot be altered by the customer or the malware infecting the PC.

The use of restricted funds transfer recipient lists or other controls over the administration of such lists, can reduce funds transfer fraud. Fraudsters must frequently add new funds transfer recipients to an account profile in order to consummate the fraud.

Overall, the Agencies agree with security experts who believe that institutions should no longer rely on one form of customer authentication. A one dimensional customer authentication program is simply not robust enough to provide the level of security that customers expect and that protects institutions from financial and reputation risk. This concept of layered security is consistent with expectations the Agencies have discussed previously.[9] Layered security controls do not have to be complex. For example, implementing time of day restrictions on the customer's authority to execute funds transfers or using

[9] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006; FFIEC IT Examination Handbook, E-Banking Booklet, August 2003.

restricted funds transfer recipient lists, in addition to robust logon authentication, can help to reduce the possibility of fraud.

The banking, payment, and security industries have continued to innovate in response to the increasing cyber threat environment. In addition to some of the control methods previously discussed, other examples of customer authentication include keystroke dynamics and biometric based responses. Additionally, institutions can look to traditional and innovative business process controls to improve security over customers' online activities. Some examples include:

- establish, require and periodically review volume and value limitations or parameters for what activities a business customer in the aggregate, and its enrolled users individually, can functionally accomplish while accessing the online system;
- monitor and alert on exception events;
- establish individual transaction and aggregate account exposure limits based on expected account activity;
- establish payee whitelisting (e.g., positive pay) and/or blacklisting;
- require every ACH file originating entity to provide a proactive notice of intent to originate a file prior to its submission; and
- require business customers to deploy dual control routines over higher risk functions performed online.