Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision

Frequently Asked Questions on

FFIEC Guidance on Authentication in an Internet Banking Environment

August 15, 2006

Purpose

The staffs of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (the Agencies) have jointly developed the attached frequently asked questions (FAQs) to assist financial institutions and their technology service providers in understanding the Federal Financial Institutions Examination Council's (FFIEC's) guidance entitled *Authentication in an Internet Banking Environment* (the guidance).

Overview

The guidance, issued on October 12, 2005, updates the FFIEC's guidance entitled *Authentication in an Electronic Banking Environment* issued in 2001. It addresses the need for risk based assessments, customer awareness, and enhanced security measures to authenticate customers using Internet-based products and services that process high risk transactions involving access to customer information or the movement of funds to other parties. The attached FAQs are a representation of questions the Agencies have received from financial institutions, Agency examiners, and technology service providers and they address the scope of the guidance, risk assessments, the time frame for implementation, and other issues.

Institutions should review these FAQs in conjunction with the guidance as they assess risks in their Internet-based products and services and determine appropriate authentication solutions for permitting access to systems that process high risk transactions involving the movement of funds to other parties or access to customer information.

Frequently Asked Questions on

FFIEC Guidance on Authentication in an Internet Banking Environment

Scope

Q-1- What was the impetus for the regulators providing guidance regarding how customers should access electronic banking systems?

A-1- Since 2001 there have been improvements in authentication technologies, increasing incidents of fraud (including identity theft), and significant legal and technological changes regarding the protection of customer information.

Q-2- Does the guidance apply to telephone banking systems?

A-2- While the guidance focuses on Internet banking systems, its principles apply to all forms of electronic banking, including telephone banking systems.

Q-3- Do the Agencies maintain a list of "approved" solutions?

A-3- No, the Agencies do not maintain a list of approved solutions.

Q-4- Is the Appendix to the guidance an "exclusive" list of solutions?

A-4- No, the Appendix is only a brief discussion of some of the technologies that the Agencies were aware of that could be used to address this issue.

Q-5- Does the guidance require the use of multifactor authentication?

A-5 No, the guidance does not call for the use of multifactor authentication. The use of multifactor authentication is one of several methods that can be used to mitigate risk as discussed in the guidance. However, the guidance identifies circumstances under which the Agencies would view the use of single-factor authentication as the only control mechanism as inadequate and conclude that additional risk mitigation is warranted.

Q-6- Does the guidance apply to both retail and commercial customers?

A-6- Yes**,** the guidance applies to both retail and commercial customers.

Q-7- Does the guidance apply to the retail use of credit and debit cards, including over the Internet?

A-7- No, the guidance does not apply to the use of credit or debit cards.

Q-8- Does the guidance apply to correspondent banking?

A-8- The guidance applies to correspondent banking if the correspondent banking relationship uses an electronic banking system with high-risk functionality as described in the guidance.

Q-9- Does the guidance specify the use of hardware tokens for authentication?

A-9 No, the use of hardware tokens is one possible method for enhancing controls surrounding the authentication of customers.

Q-10- Are the Agencies recommending multifactor authentication over layered security or other compensating controls?

A-10- No, any of these controls may be an effective method to mitigate risk in accordance with the guidance, if properly implemented.

Q-11- Are there banking applications where single-factor authentication as the only control mechanism would be adequate?

A-11- Single-factor authentication alone would be adequate for electronic banking applications that do not process high-risk transactions, e.g., systems that do not allow funds to be transferred to other parties or that do not permit access to customer information.

Q-12- Does the guidance apply to loan service companies?

A-12- The guidance applies to all financial institutions regulated by the Agencies.

Q-13- Does the guidance apply to securities brokers?

A-13- The guidance applies to the same entities and information covered by the Interagency Guidelines Establishing Information Security Standards. See ¶1.A of the Guidelines. The Securities and Exchange Commission has its own regulation on safeguarding customer information. See 17 C.F.R. 248.30.

Q-14- Can an institution perform a risk assessment and conclude that stronger authentication is not warranted?

A-14- An institution's risk assessment may conclude that existing controls are appropriate. However, such a conclusion would not be justified if the institution's electronic banking systems use single-factor authentication as their only control for high-risk transactions involving access to customer information or the movement of funds to other parties.

Q-15- If a financial institution has not experienced financial fraud or identity theft originating from its online banking system, should it nonetheless undertake risk mitigation steps in accordance with the guidance?

A-15- Yes, the guidance states that a financial institution's risk assessment should consider appropriate risk-mitigation steps for both current and future risks. (Please refer to question 14.)

Q-16- Does the guidance apply to loan or deposit account applications submitted over the Internet by non-customers?

A-16- The guidance does not apply to applications submitted by non-customers. As the appendix to the guidance explains, customer verification during account origination is a related but separate process from that of authentication.

Q-17- Does the guidance address mutual (e.g., institution-to-customer) authentication?

A-17- No, the guidance does not specifically address mutual authentication. However, mutual authentication may be an effective host authentication control mechanism and may be part of a layered security program.

Q-18- Would an institution meet the expectations of the guidance if it permits high-risk transactions through a system that relies on single-factor authentication as its only control mechanism provided that the institution chooses to reimburse customers for any losses associated with Internet fraud?

A-18- No, making customers whole for losses is not a substitute for adopting appropriate authentication measures or other controls described in the guidance.

Q-19- Does the guidance apply to call centers?

A-19- The principles of the guidance apply if a financial institution permits high-risk services to be performed through its call center.

Timing

Q-1- What do the Agencies expect institutions to have accomplished by year-end 2006?

A-1- The Agencies expect that institutions will complete the risk assessment and will implement risk mitigation activities by year-end 2006. The Agencies are not considering any general extension of the timing associated with this guidance.

Q-2- What if the financial institution or its technology service provider cannot implement a solution by year-end 2006?

A-2- The Agencies' examiners will assess the adequacy of each financial institution's authentication controls on a case-by-case basis.

Definitions

Q-1- Can you further clarify high-risk transactions involving the movement of funds to other parties and access to customer information?

A-1- The term "customer information" is defined in footnote 2 of the guidance by reference to the Interagency Guidelines Establishing Information Security Standards. Financial institutions may also want to review the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. The term "movement of funds to other parties" includes bill payment applications as well as the ability to transfer funds to a separate account maintained at the same depository institution but owned by a different party. Thus, any system that permits the movement of funds to other parties and/or the access to customer information, as defined previously, is "high-risk" necessitating stronger authentication or additional controls.

Q-2- What does the guidance mean when it refers to "layered security or other controls reasonably calculated to mitigate those risks?"

A-2 The term "layered security" includes other risk-mitigating controls that would not strictly be considered multifactor authentication. The reference to "other controls" includes other mitigating controls that exist today or that may be introduced in the future.

Risk Assessment

Q-1- What type of documentation is contemplated for the risk assessment? Do the Agencies have a template that financial institutions should use?

A-1- The guidance is not specific in this regard and the Agencies do not have a template for such risk assessments. However, financial institutions seeking general information on risk assessments may refer to the Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards and the FFIEC IT Examination Handbook, Information Security Booklet.

Q-2- Can a financial institution rely on its Internet banking system provider to perform the risk assessment?

A-2- Yes, however, the institution is ultimately responsible for managing risk and should perform appropriate due diligence as required when selecting a service provider. The institution may accept a risk assessment performed by the service provider after the institution has ensured that the assessment is accurate and the solutions are sufficient to mitigate the risks to the financial institution and its customers.

Q-3- Does the guidance provide that financial institutions will assess the risks regarding authentication on a yearly basis?

A-3 No, however the Interagency Guidelines Establishing Information Security Standards require that an institution's information security program be monitored, evaluated, and adjusted as appropriate in light of changes in technology, the sensitivity of customer information, internal and external threats to information, the institution's changing business arrangements, and changes to customer information systems. These same criteria apply to re-evaluating the institution's Internet banking controls.

Q-4- Can a financial institution forgo the risk assessment and move immediately to implement additional authentication controls?

A-4- No, because the guidance is risk-based, a risk assessment that sufficiently evaluates the risks and identifies the reasons for choosing a particular control should be completed.

Q-5- Should the risk assessment specifically consider the risks of phishing, pharming, and malware?

A-5- Yes, these are some of the vulnerabilities that are specifically mentioned in the guidance. Other factors appropriate for consideration in the risk assessment include reputation risk, harm to the customer, transaction risk, and other reasonably foreseeable threats.

Customers

Q-1- May an institution permit customers to "opt-out" of additional authentication controls?

A-1- No, the Agencies believe that permitting customers to opt-out is not an effective risk mitigation strategy and would undermine the effectiveness of the control. In addition, this would not address reputation risk to the institution. However, an institution may permit customers to choose between different authentication options provided the options offered are consistent with the guidance.

Q-2- The guidance also discusses a customer awareness program that includes periodic evaluations. How do the Agencies envision that this would be implemented?

A-2- An institution may implement a customer awareness program in a number of ways, including making information available on the institution's website, in statement stuffers or other direct mail communication, or at branch offices. The institution may track the number of times customers click on an information security hotlink or the amount of written material disseminated. The Agencies understand that institutions cannot force customers to access or read such information.

Technology Service Providers

Q-1- Will the Agencies assess the progress of technology service providers prior to year-end 2006?

A-1- The Agencies are assessing efforts being made by technology service providers to conform with the guidance as part of the ongoing interagency supervisory process.

Q-2- Should an institution rely on the authentication technique chosen by its service provider?

A-2- The institution remains ultimately responsible for the adequate authentication of transactions involving access to customer information or movement of funds to other parties. This responsibility includes ensuring that the authentication techniques chosen by its service providers are appropriate for the institution's services.

Appendix

Q-1- Would two-factor authentication include using two of the same type of factor (e.g., two different passwords) if they are used at different points in the applications?

A-1- By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication.

Q-2- Is a user logon ID considered one of the factors in multifactor authentication?

A-2- No, because user logon IDs are not secret.

Q-3- Are there authentication methods that an institution can implement without customer involvement?

A-3- An institution can implement authentication controls with varying degrees of customer involvement. Some solutions can be implemented with virtually no customer interaction while others require significantly more.