Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Federal Reserve System
Examiner Guidance

Background

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805).[1] The Guidelines apply to customer information maintained by or on behalf of state member banks and bank holding companies and their nonbank subsidiaries, except for brokers, dealers, persons providing insurance, investment companies, and investment advisors.[2] These Guidelines also apply to customer information maintained by or on behalf of Edge corporations, agreement corporations, and uninsured state-licensed branches or agencies of foreign banks.

The Guidelines require each institution to implement a *written* information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. The program should be designed to ensure the security and confidentiality of customer information, protect against unanticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. Each institution must assess risks to customer information and implement appropriate policies, procedures, training, and testing to manage and control these risks. Institutions must also report annually to the board of directors or a committee of the board of directors.

"Customer information" is defined in the Guidelines as any record, whether in paper, electronic, or other form, containing nonpublic personal information of a customer. A customer is defined in the same manner as in Regulation P--a *consumer* who has established a continuing relationship with an institution under which the institution provides one or more financial products or services to the consumer to be used primarily for personal, family, or household purposes. Customer does not include a business, nor does it include a consumer who has not established an ongoing relationship with the financial institution.

An institution or banking organization is not required to implement a *uniform* information security program. For example, a bank holding company may include subsidiaries within the scope of its information security program or the subsidiaries may implement separate information

[1] See *Federal Register* Vol. 66, No. 22, February 1, 2001, pp. 8616-8641. Also see Regulation H, 12 CFR 208, Appendix D-2; Regulation K, 12 CFR 221.9 and 221.24; and Regulation Y, 12 CFR 225, Appendix F.

[2] Separate regulations or guidelines issued by the appropriate regulatory agency regarding information security may apply to these subsidiaries.

security programs in accordance with the Guidelines. However, an institution is expected to coordinate all the elements of its information security program.

A service provider is a person or entity that maintains, processes, or otherwise is permitted access to customer information through its provisions of services directly to the bank. Institutions must exercise due diligence in selecting service providers, including reviewing the service provider's information security program or measures used by the service provider to protect the institution's customer information. In addition, contracts entered into after March 5, 2001 must require that the service provider implement appropriate measures designed to meet the objectives of the Guidelines. By July 1, 2003, all contracts are subject to this requirement.

Institutions must also conduct ongoing oversight to confirm that the service provider maintains appropriate security measures. An institution's methods for overseeing its service provider arrangements may differ depending on the type of services or service provider or the level of risk. For example, if a service provider is subject to regulations or code of conduct that impose a duty to protect customer information consistent with the objectives of the Guidelines, the institution may consider that duty in exercising its due diligence and oversight of the service provider. In situations where a service provider hires a subservicer (or subcontractor), the subservicer would not be considered a "service provider" under the Guidelines.

Examination Questionnaire

The following questionnaire may be used in assessing an institution's compliance with the Guidelines. Depending on the nature of the institution's operations and the extent of prior supervisory review, not all questions may need to be answered fully on each examination. Other examination resources may also be used if a technical evaluation of information security measures is needed.[3] Examiners should conduct sufficient review in the following areas to provide a basis for evaluating the overall information security program and compliance with the Guidelines.

1. Does the bank have a written information security program or policy? Has the written information security program been approved by the board of directors or an appropriate committee of the board?

2. Is the written information security program appropriate given the size and complexity of the organization and its operations? Does it contain the objectives of the program, assign responsibility for implementation, and provide methods for compliance and enforcement?

3. Does the bank periodically update its information security program to reflect changes in the bank's operations and systems, as well as changes in the threats or risks to the bank's customer information?

4. Review the bank's process for assessing risk to its customer information.

[3] See, for example, *FFIEC Information Systems Examination Handbook*, 1996 Edition.

a) Has the bank identified the locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information?

b) Has the bank identified reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems and assessed the likelihood and potential damage to the bank and its customers of these threats?

5. Review the bank's risk management processes for implementing effective measures to protect customer information. Does the bank consider the following areas, and adopt measures the bank concludes are appropriate based on risk?

a) Access controls on computer systems containing customer information to prevent access by unauthorized staff or other individuals.

b) Controls and procedures to prevent employees from providing customer information to unauthorized individuals, including "pretext calling."[4]

c) Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.

d) The encryption of electronic customer information, including while in transit or in storage on networks or systems, in case unauthorized individuals are able to gain access.

e) Procedures designed to ensure that modifications to customer information systems are consistent with the bank's information security program.

f) Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of internal misuse of customer information.

g) Monitoring systems and procedures to detect unauthorized access to customer information systems that could compromise the security of customer information.

h) Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[5]

i) Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

---

[4] See Federal Reserve SR Letter 01-11 "Identity Theft and Pretext Calling," April 26, 2001, for further information.
[5] See, for example, "Agencies Issues Revised Suspicious Activity Report Form (SAR)," Joint Press Release, June 19, 2000, available at http://www.federalreserve.gov/boarddocs/press/general/2000/20000619/default.htm

6. Have the bank's employees been trained to implement the information security program?

7. Does the bank regularly test the effectiveness of key controls, systems, and procedures of its information security program? This may include, for example, tests of operational contingency plans, system security audits or "penetration" tests, and tests of critical internal controls over customer information. Are tests conducted by independent staff or are test results reviewed by independent staff?

8. Does the bank provide customer information to any service providers or do any service providers have access to customer information through service provided directly to the bank?

   a) If so, has the bank conducted appropriate due diligence in selecting its service providers, taking into consideration information security?

   b) As of July 1, 2003, does the bank require its service providers by contract to implement appropriate information security programs and measures (or as of July 1, 2001 if contracts were entered into after March 5, 2001)?

   c) Where appropriate based on risk, does the bank monitor its service providers to confirm that they are maintaining appropriate security measures to safeguard the bank's customer information? For example, does the bank conduct or review the results of audits, security reviews or tests, or other evaluations?

9. Does the bank report to its board or an appropriate committee of the board at least annually on the overall status of the information security program, including the bank's compliance with the Guidelines and any other material matters?