12 CFR - CHAPTER II - PART 225

Appendix F To Part 225 -- Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Table of Contents

These 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) . These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. *Scope.* The Guidelines apply to customer information maintained by or on behalf of bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), for which the Board has supervisory authority.

B. *Preservation of Existing Authority.* These Guidelines do not in any way limit the authority of the Board to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The Board may take action under these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the Board.

C. *Definitions.* 1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p-1).

2. For purposes of the Guidelines, the following definitions apply:

a. *Board of directors*, in the case of a branch or agency of a foreign bank, means the managing official in charge of the branch or agency.

b. *Customer* means any customer of the bank holding company as defined in § 216.3(h) of this chapter.

c. *Customer information* means any record containing nonpublic personal information, as defined in § 216.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank holding company.

d. *Customer information systems* means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

e. *Service provider* means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank holding company.

f. *Subsidiary* means any company controlled by a bank holding company, except a broker, dealer, person providing insurance, investment company, investment advisor, insured depository institution, or subsidiary of an insured depository institution. II. Standards for Safeguarding Customer Information

A. *Information Security Program.* Each bank holding company shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank holding company and the nature and scope of its activities. While all parts of the bank holding company are not required to implement a uniform set of policies, all elements of the information security program must be coordinated. A bank holding company also shall ensure that each of its subsidiaries is subject to a comprehensive information security program. The bank holding company may fulfill this requirement either by including a subsidiary within the scope of the bank holding company's comprehensive information security program or by causing the

subsidiary to implement a separate comprehensive information security program in accordance with the standards and procedures in sections II and III of this appendix that apply to bank holding companies.

B. *Objectives.* A bank holding company's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. III. Development and Implementation of Information Security Program

A. *Involve the Board of Directors.* The board of directors or an appropriate committee of the board of each bank holding company shall:

1. Approve the bank holding company's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank holding company's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. *Assess Risk.* Each bank holding company shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. *Manage and Control Risk.* Each bank holding company shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank holding company's activities. Each bank holding company must consider whether the following security measures are appropriate for the bank holding company and, if so, adopt those measures the bank holding company concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

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

c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system modifications are consistent with the bank holding company's information security program;

e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the bank holding company suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. 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.

2. Train staff to implement the bank holding company's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank holding company's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. *Oversee Service Provider Arrangements.* Each bank holding company shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the bank holding company's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank holding company should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each bank holding company shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank holding company's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. *Report to the Board.* Each bank holding company shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank holding company's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. *Implement the Standards.*

1. *Effective date.* Each bank holding company must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a bank holding company has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank holding company entered into the contract on or before March 5, 2001.

[66 FR 8636, Feb. 1, 2001]