

Appendix B to Part 570—Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Table of Contents

- I. Introduction
 - A. Scope
 - B. Preservation of Existing Authority
 - C. Definitions
- II. Standards for Safeguarding Customer Information
 - A. Information Security Program
 - B. Objectives
- III. Development and Implementation of Customer Information Security Program
 - A. Involve the Board of Directors
 - B. Assess Risk
 - C. Manage and Control Risk
 - D. Oversee Service Provider Arrangements
 - E. Adjust the Program
 - F. Report to the Board
 - G. Implement the Standards

I. Introduction

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p-1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. 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 entities over which OTS has authority. For purposes of this appendix, these entities are savings associations whose deposits are FDIC-insured and any subsidiaries of such savings associations, except brokers, dealers, persons providing insurance, investment companies, and investment advisers. This appendix refers to such entities as "you".

B. *Preservation of Existing Authority.* Neither section 39 nor these Guidelines in any way limit OTS's authority to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other

practices. OTS may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to OTS.

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. *Customer* means any of your customers as defined in § 573.3(h) of this chapter.

b. *Customer information* means any record containing nonpublic personal information, as defined in § 573.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that you maintain or that is maintained on your behalf.

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

d. *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 you.

II. Standards for Safeguarding Customer Information

A. *Information Security Program.* You shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to your size and complexity and the nature and scope of your activities. While all parts of your organization are not required to implement a uniform set of policies, all elements of your information security program must be coordinated.

B. *Objectives.* Your 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.* Your board of directors or an appropriate committee of the board shall:

1. Approve your written information security program; and
2. Oversee the development, implementation, and maintenance of your information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. *Assess Risk.* You 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.* You shall:

1. Design your information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of your activities. You must consider whether the following security measures are appropriate for you and, if so, adopt those measures you conclude 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 your 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 for you to take when you suspect or detect 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 your 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 your 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.* You shall:

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

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

3. Where indicated by your risk assessment, monitor your service providers to confirm that they have satisfied their

obligations as required by paragraph D.2. As part of this monitoring, you should review audits, summaries of test results, or other equivalent evaluations of your service providers.

E. *Adjust the Program.* You shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of your customer information, internal or external threats to information, and your 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.* You shall report to your board or an appropriate committee of

the board at least annually. This report should describe the overall status of the information security program and your compliance with these Guidelines. The reports should discuss material matters related to your 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.* You 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 you have entered into with a service provider to perform services for you or functions on your behalf satisfies the provisions of paragraph 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 you entered into the contract on or before March 5, 2001.

Dated: December 19, 2000.

By the Office of Thrift Supervision.

Ellen Seidman,

Director.

[FR Doc. 01-1114 Filed 1-31-01; 8:45 am]

BILLING CODE 4810-33-P; 6210-01-P; 6714-01-P; 6720-01-P