3. The effect of growth on the institution’s capital.

G. Asset quality. An insured depository institution should establish and maintain a system that is commensurate with the institution’s size and the nature and scope of its operations to identify problem assets and prevent deterioration in those assets. The institution should:
1. Conduct periodic asset quality reviews to identify problem assets;
2. Estimate the inherent losses in those assets and establish reserves that are sufficient to absorb estimated losses;
3. Compare problem asset totals to capital;
4. Take appropriate corrective action to resolve problem assets;
5. Consider the size and potential risks of material asset concentrations; and
6. Provide periodic asset reports with adequate information for management and the board of directors to assess the level of asset risk.

H. Earnings. An insured depository institution should establish and maintain a system that is commensurate with the institution’s size and the nature and scope of its operations to evaluate and monitor earnings and ensure that earnings are sufficient to maintain adequate capital and reserves. The institution should:
1. Compare recent earnings trends relative to equity, assets, or other commonly used benchmarks to the institution’s historical results and those of its peers;
2. Evaluate the adequacy of earnings given the size, complexity, and risk profile of the institution’s assets and operations;
3. Assess the source, volatility, and sustainability of earnings, including the effect of nonrecurring or extraordinary income or expense;
4. Take steps to ensure that earnings are sufficient to maintain adequate capital and reserves after considering the institution’s asset quality and growth rate; and
5. Provide periodic earnings reports with adequate information for management and the board of directors to assess earnings performance.

I. Compensation, fees and benefits. An institution should maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the institution.

III. PROHIBITION ON COMPENSATION THAT CONSTITUTES AN UNSAFE AND UN SOUND PRACTICE

A. Excessive Compensation
Excessive compensation is prohibited as an unsafe and unsound practice. Compensation shall be considered excessive when amounts paid are unreasonable or disproportionate to the services performed by an executive officer, employee, director, or principal shareholder, considering the following:
1. The combined value of all cash and non-cash benefits provided to the individual;
2. The compensation history of the individual and other individuals with comparable expertise at the institution;
3. The financial condition of the institution;
4. Comparable compensation practices at comparable institutions, based upon such factors as asset size, geographic location, and the complexity of the loan portfolio or other assets;
5. For postemployment benefits, the projected total cost and benefit to the institution;
6. Any connection between the individual and any fraudulent act or omission, breach of trust or fiduciary duty, or insider abuse with regard to the institution; and
7. Any other factors the agencies determines to be relevant.

B. Compensation Leading to Material Financial Loss
Compensation that could lead to material financial loss to an institution is prohibited as an unsafe and unsound practice.

APPENDIX B TO PART 170—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

TABLE OF CONTENTS
I. Introduction
A. Scope
The Interagency Guidelines Establishing Information Security Standards (Guidelines) set forth standards pursuant to section 39(a) of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1), and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805(b)). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines also address standards with respect to the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w).

A. Scope. The Guidelines apply to customer information maintained by or on behalf of entities over which the OCC has authority. For purposes of this appendix, these entities are Federal 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.” These Guidelines also apply to the proper disposal of consumer information by or on behalf of such entities.

B. Preservation of Existing Authority. Neither section 39 nor these Guidelines in any way limit the OCC’s authority to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The OCC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the OCC.

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) Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by you or on your behalf for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.

(b) Aggregate information, such as the mean credit score, derived from a group of consumer reports; or

(c) Blind data, such as payment history on accounts that are not personally identifiable, that may be used for developing credit scoring models or for other purposes.

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 Information Security Standards (Guidelines) set forth standards pursuant to section 39(a) of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1), and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805(b)). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines also address standards with respect to the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w).
c. Customer means any of your customers as defined in §573.3(h) or any superseding regulation issued by the Consumer Financial Protection Bureau.

d. Customer information means any record containing nonpublic personal information, as defined in §573.3(n) or any superseding regulation issued by the Consumer Financial Protection Bureau, about a customer, whether in paper, electronic, or other form, that you maintain or that is maintained on your behalf.

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

f. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information, through its provision of services directly to you.

II. STANDARDS FOR INFORMATION SECURITY

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;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. Ensure the proper disposal of customer information and consumer information.

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.

4. Develop, implement, and maintain, as part of your information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements in this paragraph III.

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.

3. Effective date for measures relating to the disposal of consumer information. You must satisfy these Guidelines with respect to the proper disposal of consumer information by July 1, 2005.

4. Exception for existing agreements with service providers relating to the disposal of consumer information. Notwithstanding the requirement in paragraph III.G.3., your contracts with service providers that have access to consumer information and that may dispose of consumer information, entered into before July 1, 2005, must comply with the provisions of the Guidelines relating to the proper disposal of consumer information by July 1, 2006.
Supplement A to Appendix B to Part 170—Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

I. BACKGROUND

This Guidance interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines") and describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The scope of, and definitions of terms used in, this Guidance are identical to those of the Security Guidelines. For example, the term "customer information" is the same term used in the Security Guidelines, and means any record containing non-public personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution.

A. Interagency Security Guidelines

Section 501(b) of the GLBA required the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction that include administrative, technical, and physical safeguards, to protect the security and confidentiality of customer information. Accordingly, the Agencies issued Security Guidelines requiring every financial institution to have an information security program 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.

B. Risk Assessment and Controls

1. The Security Guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and

c. The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

2. Following the assessment of these risks, the Security Guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

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. Background checks for employees with responsibilities for access to customer information; and

1This Guidance was originally jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).
3See Security Guidelines, III.B.
4See Security Guidelines, III.C.
Comptroller of the Currency, Treasury

The Security Guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.6

C. Service Providers

The Security Guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.6

II. RESPONSE PROGRAM

Millions of Americans, throughout the country, have been victims of identity theft.7 Identity thieves misuse personal information they obtain from a number of sources, including financial institutions, to perpetrate identity theft. Therefore, financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial institutions should place access controls on customer information systems and conduct background checks for employees who are authorized to access customer information.8 However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems9 that occur nonetheless. A response program should be a key part of an institution’s information security program.10 The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to customer information in customer information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in the Guidelines that relate to these arrangements, and with existing guidance on this topic issued by the Agencies,11 an institution’s contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution’s customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

---

5 See Security Guidelines, III.C.
6 See Security Guidelines, III.B. and III.D. Further, the Agencies note that, in addition to contractual obligations to a financial institution, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission (“FTC”), 16 CFR part 314.
8 Institutions should also conduct background checks of employees to ensure that the institution does not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).
9 Under the Guidelines, an institution’s customer information systems consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. See Security Guidelines, I.C.2.d.
A. Components of a Response Program

1. At a minimum, an institution’s response program should contain procedures for the following:
   a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
   b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
   c. Consistent with the Agencies’ Suspicious Activity Report (“SAR”) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
   d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;13 and
   e. Notifying customers when warranted.

2. Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution’s service providers, it is the responsibility of the financial institution to notify the institution’s customers and regulator. However, an institution may authorize or contract with its service provider to notify the institution’s customers or regulator on its behalf.

III. CUSTOMER NOTICE

Financial institutions have an affirmative duty to protect their customers’ information against unauthorized access or use. Notifying customers of a security incident involving the unauthorized access or use of the customer’s information in accordance with the standard set forth below is a key part of that duty. Timely notification of customers is important to manage an institution’s reputation risk. Effective notice also may reduce an institution’s legal risk, assist in maintaining good customer relations, and enable the institution’s customers to take steps to protect themselves against the consequences of identity theft. When customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate


14 The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.
and report suspected incidents of identity theft.  

2. The Agencies encourage financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

C. Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

PART 171—FAIR CREDIT REPORTING

Subparts A–H [Reserved]

Subpart I—Duties of Users of Consumer Reports Regarding Records Disposal

§§ 171.80–170.82 [Reserved]

§ 171.83 Disposal of consumer information.

(a) Scope. This section applies to Federal savings associations whose deposits are insured by the Federal Deposit Insurance Corporation and Federal savings association operating subsidiaries in accordance with §159.3(h)(1) of this chapter (defined as “you”).

(b) In general. You must properly dispose of any consumer information that you maintain or otherwise possess in accordance with the Interagency Guidelines Establishing Information Security Standards, as set forth in appendix B to part 170, to the extent that you are covered by the scope of the Guidelines.

(c) Rule of construction. Nothing in this section shall be construed to:

(1) Require you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or

(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

Subpart J—Identity Theft Red Flags

§ 171.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Scope. This section applies to a financial institution or creditor that is a Federal savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with §159.3(h)(1) of this chapter, a Federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) Definitions. For purposes of this section and appendix J, the following definitions apply:

(1) Account means a continuing relationship established by a person with a