Title 12 —Banks and Banking
Chapter III —Federal Deposit Insurance Corporation
Subchapter B —Regulations and Statements of General Policy

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

Authority: 12 U.S.C. 1818 and 1819 (Tenth), 1831p–1; 15 U.S.C. 1681b, 1681s, 1681w, 6801(b), 6805(b)(1).

Source: 80 FR 65907, Oct. 28, 2015, unless otherwise noted.

§ 364.100 Purpose.

Section 39 of the Federal Deposit Insurance Act requires the Federal Deposit Insurance Corporation to establish safety and soundness standards. Pursuant to section 39, this part establishes safety and soundness standards by guideline.

§ 364.101 Standards for safety and soundness.

(a) ***General standards.*** The Interagency Guidelines Establishing Standards for Safety and Soundness prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1), as set forth as appendix A to this part, apply to all insured state nonmember banks, to state-licensed insured branches of foreign banks, that are subject to the provisions of section 39 of the Federal Deposit Insurance Act, and to state savings associations (in aggregate, bank or banks and savings association or savings associations).

(b) ***Interagency Guidelines Establishing Information Security Standards.*** The Interagency Guidelines Establishing Information Security Standards prescribed pursuant to section 39 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, 6805(b)), and with respect to the proper disposal of consumer information requirements pursuant to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w), as set forth in appendix B to this part, apply to all insured state nonmember banks, insured state licensed branches of foreign banks,

any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), and to state savings associations. The interagency regulations and guidelines on identity theft detection, prevention, and mitigation prescribed pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. 1681m(e), are set forth in §§ 334.90, 334.91, and appendix J of part 334.

Appendix A to Part 364—Interagency Guidelines Establishing Standards for Safety and Soundness

I. Introduction

i. Section 39 of the Federal Deposit Insurance Act[1] (FDI Act) requires each Federal banking agency (collectively, the agencies) to establish certain safety and soundness standards by regulation or by guidelines for all insured depository institutions. Under section 39, the agencies must establish three types of standards:

(1) Operational and managerial standards;

(2) compensation standards; and

(3) such standards relating to asset quality, earnings, and stock valuation as they determine to be appropriate.

ii. Section 39(a) requires the agencies to establish operational and managerial standards relating to:

(1) Internal controls, information systems and internal audit systems, in accordance with section 36 of the FDI Act (12 U.S.C. 1831m);

(2) loan documentation;

(3) credit underwriting;

(4) interest rate exposure;

(5) asset growth; and

(6) compensation, fees, and benefits, in accordance with subsection (c) of section 39. Section 39(b) requires the agencies to establish standards relating to asset quality, earnings, and stock valuation that the agencies determine to be appropriate.

iii. Section 39(c) requires the agencies to establish standards prohibiting as an unsafe and unsound practice any compensatory arrangement that would provide any executive officer, employee, director, or principal shareholder of the institution with excessive compensation, fees or benefits and any compensatory arrangement that could lead to material financial loss to an institution. Section 39(c) also requires that the agencies establish standards that specify when compensation is excessive.

iv. If an agency determines that an institution fails to meet any standard established by guidelines under subsection (a) or

(b) of section 39, the agency may require the institution to submit to the agency an acceptable plan to achieve compliance with the standard. In the event that an institution fails to submit an acceptable plan within the time allowed by the agency or fails in any material respect to implement an accepted plan, the agency must, by order, require the institution to correct the deficiency. The agency may, and in some cases must, take other supervisory actions until the deficiency has been corrected.

v. The agencies have adopted amendments to their rules and regulations to establish deadlines for submission and review of compliance plans.[2]

vi. The following Guidelines set out the safety and soundness standards that the agencies use to identify and address problems at insured depository institutions before capital becomes impaired. The agencies believe that the standards adopted in these Guidelines serve this end without dictating how institutions must be managed and operated. These standards are designed to identify potential safety and soundness concerns and ensure that action is taken to address those concerns before they pose a risk to the Deposit Insurance Fund.

A. Preservation of Existing Authority

Neither section 39 nor these Guidelines in any way limits the authority of the agencies to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. Action under section 39 and these Guidelines may be taken independently of, in conjunction with, or in addition to any other enforcement action available to the agencies. Nothing in these Guidelines limits the authority of the FDIC pursuant to section 38(i)(2)(F) of the FDI Act (12 U.S.C. 1831o) and part 324 of title 12 of the Code of Federal Regulations.

B. Definitions

1. ***In general.*** For purposes of these Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the FDI Act (12 U.S.C. 1813 and 1831p–1).
2. ***Board of directors,*** in the case of a state-licensed insured branch of a foreign bank and in the case of a federal branch of a foreign bank, means the managing official in charge of the insured foreign branch.
3. ***Compensation*** means all direct and indirect payments or benefits, both cash and non-cash, granted to or for the benefit of any executive officer, employee, director, or principal shareholder, including but not limited to payments or benefits derived from an employment contract, compensation or benefit agreement, fee arrangement, perquisite, stock option plan, postemployment benefit, or other compensatory arrangement.
4. ***Director*** shall have the meaning described in 12 CFR 215.2(d).[3]
5. ***Executive officer*** shall have the meaning described in 12 CFR 215.2(e).[4]
6. ***Principal shareholder*** shall have the meaning described in 12 CFR 215.2(m).[5]

II. Operational and Managerial Standards

A. ***Internal controls and information systems.*** An institution should have internal controls and information systems that are appropriate to the size of the institution and the nature, scope and risk of its activities and that provide for:

1. An organizational structure that establishes clear lines of authority and responsibility for monitoring adherence to established policies;
2. Effective risk assessment;
3. Timely and accurate financial, operational and regulatory reports;
4. Adequate procedures to safeguard and manage assets; and
5. Compliance with applicable laws and regulations.

B. ***Internal audit system.*** An institution should have an internal audit system that is appropriate to the size of the institution and the nature and scope of its activities and that provides for:

1. Adequate monitoring of the system of internal controls through an internal audit function. For an institution whose size, complexity or scope of operations does not warrant a full scale internal audit function, a system of independent reviews of key internal controls may be used;
2. Independence and objectivity;
3. Qualified persons;
4. Adequate testing and review of information systems;
5. Adequate documentation of tests and findings and any corrective actions;
6. Verification and review of management actions to address material weaknesses; and

7. Review by the institution's audit committee or board of directors of the effectiveness of the internal audit systems.

C. ***Loan documentation.*** An institution should establish and maintain loan documentation practices that:

1. Enable the institution to make an informed lending decision and to assess risk, as necessary, on an ongoing basis;

2. Identify the purpose of a loan and the source of repayment, and assess the ability of the borrower to repay the indebtedness in a timely manner;

3. Ensure that any claim against a borrower is legally enforceable;

4. Demonstrate appropriate administration and monitoring of a loan; and

5. Take account of the size and complexity of a loan.

D. ***Credit underwriting.*** An institution should establish and maintain prudent credit underwriting practices that:

1. Are commensurate with the types of loans the institution will make and consider the terms and conditions under which they will be made;

2. Consider the nature of the markets in which loans will be made;

3. Provide for consideration, prior to credit commitment, of the borrower's overall financial condition and resources, the financial responsibility of any guarantor, the nature and value of any underlying collateral, and the borrower's character and willingness to repay as agreed;

4. Establish a system of independent, ongoing credit review and appropriate communication to management and to the board of directors;

5. Take adequate account of concentration of credit risk; and

6. Are appropriate to the size of the institution and the nature and scope of its activities.

E. ***Interest rate exposure.*** An institution should:

1. Manage interest rate risk in a manner that is appropriate to the size of the institution and the complexity of its assets and liabilities; and

2. Provide for periodic reporting to management and the board of directors regarding interest rate risk with adequate information for management and the board of directors to assess the level of risk.

F. ***Asset growth.*** An institution's asset growth should be prudent and consider:

1. The source, volatility and use of the funds that support asset growth;

2. Any increase in credit risk or interest rate risk as a result of growth; and

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 Unsound 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 noncash 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 determine 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.

[1] Section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1) was added by section 132 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), Pub. L. 102–242, 105 Stat. 2236 (1991), and amended by section 956 of the Housing and Community Development Act of 1992, Pub. L. 102–550, 106 Stat. 3895 (1992) and section 318 of the Riegle Community Development and Regulatory Improvement Act of 1994, Pub. L. 103–325, 108 Stat. 2160 (1994).

[2] For the Office of the Comptroller of the Currency, these regulations appear at 12 CFR Part 30; for the Board of Governors of the Federal Reserve System, these regulations appear at 12 CFR Part 263; and for the Federal Deposit Insurance Corporation, these regulations appear at 12 CFR Part 308, subpart R.

[3] In applying these definitions for savings associations, pursuant to 12 U.S.C. 1464, savings associations shall use the terms “savings association” and “insured savings association” in place of the terms “member bank” and “insured bank”.

[4] See footnote 3 in section I.B.4. of this appendix.

[5] See footnote 3 in section I.B.4. of this appendix.

[80 FR 65907, Oct. 28, 2015, as amended at 83 FR 17742, Apr. 24, 2018]

Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards

Table of Contents

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 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p–1, and sections 501 and 505(b), 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. 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, and to the disposal of consumer information by or on the behalf of, entities over which the Federal Deposit Insurance Corporation (FDIC) has authority. Such entities, referred to as "insured depository institution" or "institution" are banks insured by the FDIC (other than members of the Federal Reserve System), state savings associations insured by the FDIC, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

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

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. ***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 or on behalf of the institution for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not personally identify an individual.

i. ***Examples:***

(1) ***Consumer information*** includes:

(A) A consumer report that an institution obtains;

(B) information from a consumer report that the institution obtains from its affiliate after the consumer has been given a notice and has elected not to opt out of that sharing;

(C) information from a consumer report that the institution obtains about an individual who applies for but does not receive a loan, including any loan sought by an individual for a business purpose;

(D) information from a consumer report that the institution obtains about an individual who guarantees a loan (including a loan to a business entity); or

(E) information from a consumer report that the institution obtains about an employee or prospective employee.

(2) ***Consumer information*** does not include:

(A) aggregate information, such as the mean score, derived from a group of consumer reports; or

(B) 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.

c. ***Consumer report*** has the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681a(d).

d. ***Customer*** means any customer of the institution as defined in § 332.3(h) of this chapter.

e. ***Customer information*** means any record containing nonpublic personal information, as defined in § 332.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the institution.

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

g. ***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 the institution.

II. Standards for Information Security

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

B. ***Objectives.*** An institution'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;

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.*** The board of directors or an appropriate committee of the board of each insured depository institution shall:

1. Approve the institution's written information security program; and

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

B. ***Assess Risk.***

Each institution 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 institution 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 institution's activities. Each institution must consider whether the following security measures are appropriate for the institution and, if so, adopt those measures the institution 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 institution'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 institution 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 institution'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 institution'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.

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

D. ***Oversee Service Provider Arrangements.*** Each institution 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 institution'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, an institution should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. ***Adjust the Program.*** Each institution 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 institution'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 institution 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 institution's compliance with these Guidelines. The report, which will vary depending upon the complexity of each institution's program 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 institution 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 an institution has entered into with a service provider to perform services for it or functions on its 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 the institution entered into the contract on or before March 5, 2001.

3. ***Effective date for measures relating to the disposal of consumer information.*** Each institution 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., an institution's contracts with its 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 364 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

I. Background

This Guidance[1] interprets section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information Security Standards (the Security Guidelines)[2] 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 nonpublic 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.[3]
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,[4] 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
    c. Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[5]

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 customers.[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 systems[9] 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.

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,[12] 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 institutions' 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 law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

1. Sensitive Customer Information

Under the Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is most likely to be misused, as in the commission of identity theft. For purposes of this Guidance, *sensitive customer information* means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. *Sensitive customer information* also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number.

2. Affected Customers

If a financial institution, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the institution determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

B. Content of Customer Notice

1. Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it

should include a telephone number that customers can call for further information and assistance.[14] The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identify theft to the institution. The notice should include the following additional items, when appropriate:

a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;

b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;

c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the customer may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.[15]

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 email address and who have agreed to receive communications electronically.

[1] This Guidance was jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). Pursuant to 12 U.S.C. 5412, the OTS is no longer a party to this Guidance.

[2] 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D–2 and part 225, app. F (Board); and 12 CFR part 364, app. B (FDIC). The "Interagency Guidelines Establishing Information Security Standards" were formerly known as "The Interagency Guidelines Establishing Standards for Safeguarding Customer Information."

[3] *See* Security Guidelines, III.B.

[4] *See* Security Guidelines, III.C.

[5] *See* Security Guidelines, III.C.

[6] *See* Security Guidelines, II.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), 12 CFR part 314.

[7] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identity theft in 2002. *See* The Federal Trade Commission. *Identity Theft Survey Report* (September 2003), available at *http://www.ftc.gov/os/2003/09/synovatereport.pdf*.

[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.

[10] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002 available at *http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.* Federal Reserve SR 97–32, Sound Practice Guidance for Information Security for Networks, Dec. 4, 1997; OCC Bulletin 2000–14, “Infrastructure Threats—Intrusion Risks” (May 15, 2000), for additional guidance on preventing, detecting, and responding to intrusions into financial institutions computer systems.

[11] *See* Federal Reserve SR Ltr. 13-19, Guidance on Managing Outsourcing Risk, Dec. 5, 2013; OCC Bulletin 2013–29, “Third-Party Relationships—Risk Management Guidance,” Oct. 30, 2013; and FDIC FIL 44–08, Guidance for Managing Third Party Risk, June 6, 2008 and FIL 68–99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999.

[12] An institution's obligations to file a SAR is set out in the Agencies' SAR regulations and Agency guidance. *See, for example, 12 CFR 21.11* (national banks, Federal branches and agencies); 12 CFR 163.180 (Federal savings associations); 12 CFR 208.62 (State member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured State branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); and 12 CFR part 353 (FDIC-supervised institutions). National banks must file SARs in connection with computer intrusions and other computer crimes. *See* OCC Bulletin 2000–14, “Infrastructure Threats—Intrusion Risks” (May 15, 2000); Advisory Letter 97–9, “Reporting Computer Related Crimes” (November 19, 1997) (general guidance still applicable though instructions for new SAR form published in 65 FR 1229, 1230 (January 7, 2000)). *See also* Federal Reserve SR 01–11, Identity Theft and Pretext Calling, Apr. 26, 2001.

[13] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002, pp. 68–74.

[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.

15 Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.consumer.gov/idtheft* and 1–877–IDTHEFT. The institution may also refer customers to any materials developed pursuant to section 151(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).