

[58 FR 31335, June 2, 1993, as amended at 61 FR 6494, Feb. 21, 1996; 62 FR 63258, Nov. 28, 1997]

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

Sec.

364.100 Purpose.

364.101 Standards for safety and soundness.

APPENDIX A TO PART 364—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFETY AND SOUNDNESS

APPENDIX B TO PART 364—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

AUTHORITY: 12 U.S.C. 1819(Tenth), 1831p-1; 15 U.S.C. 6801(b), 6805(b)(1).

SOURCE: 60 FR 35685, July 10, 1995, 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 and to state-licensed insured branches of foreign banks, that are subject to the provisions of section 39 of the Federal Deposit Insurance Act.

(b) *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.* The Interagency Guidelines Establishing Standards for Safeguarding Customer Information 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)), as set forth in appendix B to this part, apply to all insured state nonmember banks, insured state licensed branches of foreign banks, and any subsidiaries of such en-

titles (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

[63 FR 55488, Oct. 15, 1998, as amended at 66 FR 8638, Feb. 1, 2001]

APPENDIX A TO PART 364—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFETY AND SOUNDNESS

TABLE OF CONTENTS

I. Introduction

- A. Preservation of existing authority.
- B. Definitions.

II. Operational and Managerial Standards

- A. Internal controls and information systems.
- B. Internal audit system.
- C. Loan documentation.
- D. Credit underwriting.
- E. Interest rate exposure.
- F. Asset growth.
- G. Asset quality.
- H. Earnings.
- I. Compensation, fees and benefits.

III. Prohibition on Compensation That Constitutes an Unsafe and Unsound Practice

- A. Excessive compensation.
- B. Compensation leading to material financial loss.

I. INTRODUCTION

i. Section 39 of the Federal Deposit Insurance Act¹ (FDI Act) requires each Federal banking agency (collectively, the agencies) to establish certain safety and soundness standards by regulation or by guideline 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

¹Section 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).

(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 guideline 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 funds.

²For 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; for the Federal Deposit Insurance Corporation, these regulations appear at 12 CFR Part 308, subpart R, and for the Office of Thrift Supervision, these regulations appear at 12 CFR Part 570.

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. 1831(o)) and Part 325 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(c).³

5. *Executive officer* shall have the meaning described in 12 CFR 215.2(d).⁴

6. *Principal shareholder* shall have the meaning described in 12 CFR 215.2(j).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:

³In 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”.

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

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

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 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 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.

[60 FR 35678, 35685, July 10, 1995; 61 FR 43951, Aug. 27, 1996]

APPENDIX B TO PART 364—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 the Federal Deposit Insurance Corporation (FDIC) has authority. Such entities, referred to as "the bank" are banks insured by the FDIC (other than members of the Federal Reserve System), 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. *Customer* means any customer of the bank as defined in §332.3(h) of this chapter.

c. *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 bank.

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.

II. STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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

B. *Objectives.* A bank'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 shall:

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

B. *Assess Risk.*

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

Pt. 365

12 CFR Ch. III (1-1-04 Edition)

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'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 should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each bank 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'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 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's compliance with these Guidelines. The report, which will vary depending upon the complexity of each bank'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 bank 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 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 bank entered into the contract on or before March 5, 2001.

[66 FR 8638, Feb. 1, 2001]

PART 365—REAL ESTATE LENDING STANDARDS

Sec.

365.1 Purpose and scope.

365.2 Real estate lending standards.

APPENDIX A TO PART 365—INTERAGENCY GUIDELINES FOR REAL ESTATE LENDING POLICIES

AUTHORITY: 12 U.S.C. 1828(o).

SOURCE: 57 FR 62896, 62900, Dec. 31, 1992, unless otherwise noted.

§365.1 Purpose and scope.

This part, issued pursuant to section 304 of the Federal Deposit Insurance Corporation Improvement Act of 1991, 12 U.S.C. 1828(o), prescribes standards for real estate lending to be used by insured state nonmember banks (including state-licensed insured branches of foreign banks) in adopting internal real estate lending policies.

§365.2 Real estate lending standards.

(a) Each insured state nonmember bank shall adopt and maintain written policies that establish appropriate limits and standards for extensions of credit that are secured by liens on or interests in real estate, or that are made for the purpose of financing permanent improvements to real estate.

(b)(1) Real estate lending policies adopted pursuant to this section must:

(i) Be consistent with safe and sound banking practices;

(ii) Be appropriate to the size of the institution and the nature and scope of its operations; and

(iii) Be reviewed and approved by the bank's board of directors at least annually.

(2) The lending policies must establish:

(i) Loan portfolio diversification standards;

(ii) Prudent underwriting standards, including loan-to-value limits, that are clear and measurable;

(iii) Loan administration procedures for the bank's real estate portfolio; and

(iv) Documentation, approval, and reporting requirements to monitor compliance with the bank's real estate lending policies.

(c) Each insured state nonmember bank must monitor conditions in the real estate market in its lending area to ensure that its real estate lending policies continue to be appropriate for current market conditions.

(d) The real estate lending policies adopted pursuant to this section should