

§ 570.5

(iii) Any other relevant information, mitigating circumstances, documentation, or other evidence in support of the position of the savings association regarding the proposed order.

(d) *OTS consideration of response.* After considering the response, the OTS may:

(1) Issue the order as proposed or in modified form;

(2) Determine not to issue the order and so notify the savings association; or

(3) Seek additional information or clarification of the response from the savings association, or any other relevant source.

(e) *Failure to file response.* Failure by a savings association to file with the OTS, within the specified time period, a written response to a proposed order shall constitute a waiver of the opportunity to respond and shall constitute consent to the issuance of the order.

(f) *Request for modification or rescission of order.* Any savings association that is subject to an order under this subpart may, upon a change in circumstances, request in writing that the OTS reconsider the terms of the order, and may propose that the order be rescinded or modified. Unless otherwise ordered by the OTS, the order shall continue in place while such request is pending before the OTS.

§ 570.5 Enforcement of orders.

(a) *Judicial remedies.* Whenever a savings association fails to comply with an order issued under section 39 of the FDI Act, the OTS may seek enforcement of the order in the appropriate United States district court pursuant to section 8(i)(1) of the FDI Act.

(b) *Administrative remedies.* Pursuant to section 8(i)(2)(A) of the FDI Act, the OTS may assess a civil money penalty against any savings association that violates or otherwise fails to comply with any final order issued under section 39 and against any savings association-affiliated party who participates in such violation or noncompliance.

(c) *Other enforcement action.* In addition to the actions described in paragraphs (a) and (b) of this section, the OTS may seek enforcement of the provisions of section 39 of the FDI Act or

12 CFR Ch. V (1–1–06 Edition)

this part through any other judicial or administrative proceeding authorized by law.

APPENDIX A TO PART 570—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFETY AND SOUNDNESS

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 (12 U.S.C. 1831m); (2) loan documentation; (3) credit underwriting; (4) interest rate exposure; (5) asset growth; and (6) compensation.

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).

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.

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,

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.

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(l).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

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.

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, 35687, July 10, 1995, as amended at 61 FR 43952, Aug. 27, 1996]

APPENDIX B TO PART 570—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

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 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 OTS has authority. For purposes of this appendix, these entities are savings associations whose deposits are FDIC-insured and any subsidiaries of such savings associations, except brokers, dealers, persons providing insurance, investment companies, and investment advisers. This appendix refers to such entities as "you". 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 OTS's authority to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. OTS may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to OTS.

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

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

a. *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.

i. *Examples.* (1) *Consumer information* includes:

- (A) A consumer report that a savings association obtains;
- (B) Information from a consumer report that you obtain from your affiliate after the