(ILSA) a banking institution shall submit to the OCC, at least quarterly, information regarding the amounts and composition of its holdings of international assets.

(2) Pursuant to section 907(b) of ILSA (12 U.S.C. 3906), a banking institution shall submit to the OCC information regarding concentrations in its holdings of international assets that are material in relation to total assets and to capital of the institution, such information to be made publicly available by the OCC on request.

(b) *Procedures.* The format, content, and reporting and filing dates of the reports required under paragraph (a) of this section shall be determined jointly by the Federal banking agencies. The requirements to be prescribed by the agencies may include changes to existing reporting forms (such as the Country Exposure Report, FFIEC 009) or such other requirements as the agencies deem appropriate. The agencies also may determine to exempt from the requirements of paragraph (a) of this section banking institutions that, in the agencies' judgment, have *de minimis* holdings of international assets.

(c) *Reservation of authority.* Nothing contained in this part shall preclude the OCC from requiring from a banking institution such additional or more frequent information on the institution's holdings of international assets as the OCC may consider necessary.

PART 29 [RESERVED]

PART 30—SAFETY AND SOUNDNESS STANDARDS

Sec.

AUTHORITY: 12 U.S.C. 1, 93a, 371, 1462a, 1463, 1464, 1467a, 1818, 1828, 1831p-1, 1881–1884, 3102(b) and 5412(b)(2)(B); 15 U.S.C. 1681s, 1681w, 6801, and 6805(b)(1).

SOURCE: 60 FR 35680, July 10, 1995, unless otherwise noted.

EDITORIAL NOTE: Nomenclature changes to part 30 appear at 69 FR 77616, Dec. 28, 2004.

§ 30.1 Scope.

(a) The rules set forth in this part and the standards set forth in appendices A, B, C, and D to this part apply to national banks, Federal savings associations, and Federal branches of foreign banks that are subject to the provisions of section 39 of the Federal Deposit Insurance Act (section 39)(12 U.S.C. 1831p–1).

(b) The standards set forth in appendix B to this part also apply to uninsured national banks, Federal branches and Federal agencies of foreign banks, and the subsidiaries of any national bank, Federal savings association, and Federal branch and Federal agency of a foreign bank (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). Violation of these standards may be an unsafe and unsound practice within the meaning of 12 U.S.C. 1818.

[66 FR 8633, Feb. 1, 2001, as amended at 70 FR 6332, Feb. 7, 2005; 79 FR 54543, Sept. 11, 2014]

§ 30.2 Purpose.

Section 39 of the FDI Act, 12 U.S.C. 1831p–1, requires the Office of the Comptroller of the Currency (OCC) to establish safety and soundness standards. Pursuant to section 39, a national bank or Federal savings association may be required to submit a compliance plan if it is not in compliance with a safety and soundness standard prescribed by guideline under section 39(a) or (b). An enforceable order under section 8 of the FDI Act, 12 U.S.C.

1818(b), may be issued if, after being notified that it is in violation of a safety and soundness standard prescribed under section 39, the national bank or Federal savings association fails to submit an acceptable compliance plan or fails in any material respect to implement an accepted plan. This part establishes procedures for requiring submission of a compliance plan and issuing an enforceable order pursuant to section 39. The Interagency Guidelines Establishing Standards for Safety and Soundness are set forth in appendix A to this part, and the Interagency Guidelines Establishing Information Security Standards are set forth in appendix B to this part. The OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices are set forth in appendix C to this part. The OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches are set forth in appendix D to this part.

[60 FR 35680, July 10, 1995, as amended at 63 FR 55488, Oct. 15, 1998; 64 FR 52641, Sept. 30, 1999; 66 FR 8633, Feb. 1, 2001; 70 FR 6332, Feb. 7, 2005; 79 FR 54543, Sept. 11, 2014]

§ 30.3 Determination and notification of failure to meet safety and soundness standards and request for compliance plan.

(a) *Determination.* The OCC may, based upon an examination, inspection, or any other information that becomes available to the OCC, determine that a national bank or Federal savings association has failed to satisfy the safety and soundness standards contained in the Interagency Guidelines Establishing Standards for Safety and Soundness set forth in appendix A to this part, the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part, the OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices set forth in appendix C to this part, or the OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches set forth in appendix D to this part.

(b) *Request for compliance plan.* If the OCC determines that a national bank or Federal savings association has failed to satisfy a safety and soundness standard pursuant to paragraph (a) of this section, the OCC may request, by letter or through a report of examination, the submission of a compliance plan and the bank or savings association shall be deemed to have notice of the deficiency three days after mailing of the letter by the OCC or delivery of the report of examination.

[60 FR 35680, July 10, 1995, as amended at 63 FR 55488, Oct. 15, 1998; 64 FR 52641, Sept. 30, 1999; 66 FR 8633, Feb. 1, 2001; 70 FR 6332, Feb. 7, 2005; 79 FR 54543, Sept. 11, 2014]

§ 30.4 Filing of safety and soundness compliance plan.

(a) *Schedule for filing compliance plan*—(1) *In general.* A national bank or Federal savings association shall file a written safety and soundness compliance plan with the OCC within 30 days of receiving a request for a compliance plan pursuant to §30.3(b) unless the OCC notifies the bank or savings association in writing that the plan is to be filed within a different period.

(2) *Other plans.* If a national bank or Federal savings association is obligated to file, or is currently operating under, a capital restoration plan submitted pursuant to section 38 of the FDI Act (12 U.S.C. 1831o), a cease-and-desist order entered into pursuant to section 8 of the FDI Act (12 U.S.C. 1818(b)), a formal or informal agreement, or a response to a report of examination or report of inspection, it may, with the permission of the OCC, submit a compliance plan under this section as part of that plan, order, agreement, or response, subject to the deadline provided in paragraph (a) of this section.

(b) *Contents of plan.* The compliance plan shall include a description of the steps the national bank or Federal savings association will take to correct the deficiency and the time within which those steps will be taken.

(c) *Review of safety and soundness compliance plans.* Within 30 days after receiving a safety and soundness compliance plan under this part, the OCC

shall provide written notice to the national bank or Federal savings association of whether the plan has been approved or seek additional information from the bank or savings association regarding the plan. The OCC may extend the time within which notice regarding approval of a plan will be provided.

(d) *Failure to submit or implement a compliance plan*—(1) *Supervisory actions.* If a national bank or Federal savings association fails to submit an acceptable plan within the time specified by the OCC or fails in any material respect to implement a compliance plan, then the OCC shall, by order, require the bank or savings association to correct the deficiency and may take further actions provided in section 39(e)(2)(B). Pursuant to section 39(e)(3), the OCC may be required to take certain actions if the national bank or Federal savings association commenced operations or experienced a change in control within the previous 24-month period, or the bank or savings association experienced extraordinary growth during the previous 18-month period.

(2) *Extraordinary growth.* For purposes of paragraph (d)(1) of this section, extraordinary growth means an increase in assets of more than 7.5 percent during any quarter within the 18-month period preceding the issuance of a request for submission of a compliance plan, by a national bank or Federal savings association that is not well capitalized for purposes of section 38 of the FDI Act. For purposes of calculating an increase in assets, assets acquired through merger or acquisition approved pursuant to the Bank Merger Act (12 U.S.C. 1828(c)) will be excluded.

(e) *Amendment of compliance plan.* A national bank or Federal savings association that has filed an approved compliance plan may, after prior written notice to and approval by the OCC, amend the plan to reflect a change in circumstance. Until such time as a proposed amendment has been approved, the bank or savings association shall implement the compliance plan as previously approved.

[60 FR 35680, July 10, 1995, as amended at 79 FR 54543, Sept. 11, 2014]

§ 30.5 Issuance of orders to correct deficiencies and to take or refrain from taking other actions.

(a) *Notice of intent to issue order*—(1) *In general.* The OCC shall provide a national bank or Federal savings association prior written notice of the OCC's intention to issue an order requiring the bank or savings association to correct a safety and soundness deficiency or to take or refrain from taking other actions pursuant to section 39 of the FDI Act. The national bank or Federal savings association shall have such time to respond to a proposed order as provided by the OCC under paragraph (c) of this section.

(2) *Immediate issuance of final order.* If the OCC finds it necessary in order to carry out the purposes of section 39 of the FDI Act, the OCC may, without providing the notice prescribed in paragraph (a)(1) of this section, issue an order requiring a national bank or Federal savings association immediately to take actions to correct a safety and soundness deficiency or take or refrain from taking other actions pursuant to section 39. A national bank or Federal savings association that is subject to such an immediately effective order may submit a written appeal of the order to the OCC. Such an appeal must be received by the OCC within 14 calendar days of the issuance of the order, unless the OCC permits a longer period. The OCC shall consider any such appeal, if filed in a timely manner, within 60 days of receiving the appeal. During such period of review, the order shall remain in effect unless the OCC, in its sole discretion, stays the effectiveness of the order.

(b) *Content of notice.* A notice of intent to issue an order shall include:

(1) A statement of the safety and soundness deficiency or deficiencies that have been identified at the national bank or Federal savings association;

(2) A description of any restrictions, prohibitions, or affirmative actions that the OCC proposes to impose or require;

(3) The proposed date when such restrictions or prohibitions would be effective or the proposed date for completion of any required action; and

(4) The date by which the national bank or Federal savings association subject to the order may file with the OCC a written response to the notice.

(c) *Response to notice*—(1) *Time for response.* A national bank or Federal savings association may file a written response to a notice of intent to issue an order within the time period set by the OCC. Such a response must be received by the OCC within 14 calendar days from the date of the notice unless the OCC determines that a different period is appropriate in light of the safety and soundness of the national bank or Federal savings association or other relevant circumstances.

(2) *Content of response.* The response should include:

(i) An explanation why the action proposed by the OCC is not an appropriate exercise of discretion under section 39;

(ii) Any recommended modification of the proposed order; and

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

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

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

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

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

(e) *Failure to file response.* Failure by a national bank or Federal savings association to file with the OCC, 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 national bank or Federal savings association that is subject to an order under this part may, upon a change in circumstances, request in writing that the OCC reconsider the terms of the order, and may propose that the order be rescinded or modified. Unless otherwise ordered by the OCC, the order shall continue in place while such request is pending before the OCC.

[60 FR 35680, July 10, 1995, as amended at 79 FR 54544, Sept. 11, 2014]

§ 30.6 Enforcement of orders.

(a) *Judicial remedies.* Whenever a national bank or Federal savings association fails to comply with an order issued under section 39, the OCC may seek enforcement of the order in the appropriate United States district court pursuant to section 8(i)(1) of the FDI Act, 12 U.S.C. 1818(i)(1).

(b) *Failure to comply with order.* Pursuant to section 8(i)(2)(A) of the FDI Act, 12 U.S.C. 1818(i)(2)(A), the OCC may assess a civil money penalty against any national bank or Federal savings association that violates or otherwise fails to comply with any final order issued under section 39 and against any institution-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 OCC may seek enforcement of the provisions of section 39 or this part through any other judicial or administrative proceeding authorized by law.

[60 FR 35680, July 10, 1995, as amended at 79 FR 54544, Sept. 11, 2014]

APPENDIX A TO PART 30—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFETY AND SOUNDNESS

TABLE OF CONTENTS

B. Compensation leading to material financial loss.

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 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, 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, 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,

[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 and 12 CFR part 391, subpart B.

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

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 assetquality reviews to identify problem assets;

---

[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.

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 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.

[60 FR 35678, 35682, July 10, 1995, as amended at 61 FR 43950, Aug. 27, 1996; 79 FR 54544, Sept. 11, 2014]

Appendix B to Part 30—Interagency Guidelines Establishing Information Security Standards

Table of Contents

I. Introduction

The Interagency Guidelines Establishing Information Security Standards (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. 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. Such entities, referred to as ''the national

bank or Federal savings association,'' are national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). The 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 authority of the OCC 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. *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 national bank or Federal savings association 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 national bank or Federal savings association obtains;

(B) Information from a consumer report that the national bank or Federal savings association 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 national bank or Federal savings association 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 national bank or Federal savings association obtains about an individual who guarantees a loan (including a loan to a business entity); or

(E) Information from a consumer report that the national bank or Federal savings association obtains about an employee or prospective employee.

(2) *Consumer information* does not include:

(A) Aggregate information, such as the mean credit 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 national bank or Federal savings association as defined in 12 CFR 1016.3(i).

e. *Customer information* means any record containing nonpublic personal information, as defined in 12 CFR 1016.3(p), about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the national bank or Federal savings association.

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 national bank or Federal savings association.

II. Standards for Information Security

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

B. *Objectives.* A national bank's or Federal savings association'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 national bank or Federal savings association shall:

1. Approve the national bank's or Federal savings association's written information security program; and

2. Oversee the development, implementation, and maintenance of the national bank's or Federal savings association's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. *Assess Risk.* Each national bank or Federal savings association 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 national bank or Federal savings association 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 national bank's or Federal savings association's activities. Each national bank or Federal savings association must consider whether the following security measures are appropriate for the national bank or Federal savings association and, if so, adopt those measures the national bank or Federal savings association 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 national bank's or Federal savings association'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 national bank or Federal savings association 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 national bank's or Federal savings association'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 national bank's or Federal savings association'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 national bank or Federal savings association 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 national bank's or Federal savings association's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by section D.2. As part of this monitoring, a national bank or Federal savings association should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each national bank or Federal savings association 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 national bank's or Federal savings association'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 national bank or Federal savings association 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 national

bank's or Federal savings association's compliance with these Guidelines. The reports 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 national bank or Federal savings association 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 national bank or Federal savings association has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section 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 national bank or Federal savings association entered into the contract on or before March 5, 2001.

3. *Effective date for measures relating to the disposal of consumer information.* Each national bank or Federal savings association 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., a national bank's or Federal savings association'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 30—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]

[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 and 12 CFR 391.5 (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.

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 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 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

[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''), 16 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://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm.* 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 institution 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 68–99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999.

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 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 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,

[12] An institution's obligation to file a SAR is set out in the Agencies' SAR regulations and Agency guidance. *See* 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); 12 CFR part 353 (State non-member banks); and 12 CFR 390.355 (state savings associations). National banks and Federal savings associations must file SARs in connection with computer intrusions and other computer crimes. *See* OCC Bulletin 2000–14, ''Infrastructure Threats—Intrusion Risks'' (May 15, 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.

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 and 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 identity 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 e-mail address and who have agreed to receive communications electronically.

[66 FR 8633, Feb. 1, 2001, as amended at 69 FR 77616, Dec. 28, 2004; 70 FR 15751, 15753, Mar. 29, 2005; 71 FR 5780, Feb. 3, 2006; 79 FR 54544, Sept. 11, 2014]

APPENDIX C TO PART 30—OCC GUIDELINES ESTABLISHING STANDARDS FOR RESIDENTIAL MORTGAGE LENDING PRACTICES

TABLE OF CONTENTS

[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).

I. INTRODUCTION

i. These OCC Guidelines for Residential Mortgage Lending Practices (Guidelines) set forth standards pursuant to Section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p–1 (Section 39). The Guidelines are designed to protect against involvement by national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and their respective operating subsidiaries (together, ''national banks and Federal savings associations''), either directly or through loans that they purchase or make through intermediaries, in predatory or abusive residential mortgage lending practices that are injurious to their respective customers and that expose the national bank or Federal savings association to credit, legal, compliance, reputation, and other risks. The Guidelines focus on the substance of activities and practices, not the creation of policies. The Guidelines are enforceable under Section 39 in accordance with the procedures prescribed by the regulations in 12 CFR part 30.

ii. As the OCC has previously indicated in guidance to national banks and in rulemaking proceedings (OCC Advisory Letters 2003–2 and 2003–3 (Feb. 21, 2003)), many of the abusive practices commonly associated with predatory mortgage lending, such as loan flipping and equity stripping, will involve conduct that likely violates the Federal Trade Commission Act's (FTC Act) prohibition against unfair or deceptive acts or practices. 15 U.S.C. 45. In addition, loans that involve violations of the FTC Act, or mortgage loans based predominantly on the foreclosure or liquidation value of the borrower's collateral without regard to the borrower's ability to repay the loan according to its terms, will involve violations of OCC regulations governing real estate lending activities, 12 CFR 34.3 (Lending Rules).

iii. In addition, national banks, Federal savings associations, and their respective operating subsidiaries must comply with the requirements and Guidelines affecting appraisals of residential mortgage loans and appraiser independence. 12 CFR part 34, subpart C, and the Interagency Appraisal and Evaluation Guidelines (OCC Bulletin 2010–42 (December 10, 2010). For example, engaging in a practice of influencing the independent judgment of an appraiser with respect to a valuation of real estate that is to be security for a residential mortgage loan would violate applicable standards.

iv. Targeting inappropriate credit products and unfair loan terms to certain borrowers also may entail conduct that violates the FTC Act, as well as the Equal Credit Opportunity Act (ECOA) and the Fair Housing Act (FHA). 15 U.S.C. 1691 *et seq.* 42 U.S.C. 3601 *et seq.* For example, ''steering'' a consumer to a loan with higher costs rather than to a comparable loan offered by the national bank or Federal savings association with lower costs for which the consumer could qualify, on a prohibited basis such as the borrower's race, national origin, age, gender, or marital status, would be unlawful.

v. OCC regulations also prohibit national banks and their operating subsidiaries from providing lump sum, single premium fees for debt cancellation contracts and debt suspension agreements in connection with residential mortgage loans. 12 CFR 37.3(c)(2). Some lending practices and loan terms, including financing single premium credit insurance and the use of mandatory arbitration clauses, also may significantly impair the eligibility of a residential mortgage loan for purchase in the secondary market.

vi. Finally, OCC regulations and supervisory guidance on fiduciary activities and asset management address the need for national banks and Federal savings associations to perform due diligence and exercise appropriate control with regard to trustee activities. *See* 12 CFR 9.6 (a), in the case of national banks, and 12 CFR 150.200, in the case of Federal savings associations, and the Comptroller's Handbook on Asset Management. For example, national banks and Federal savings associations should exercise appropriate diligence to minimize potential reputation risks when they undertake to act as trustees in mortgage securitizations.

A. *Scope.* These Guidelines apply to the residential mortgage lending activities of national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and operating 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 limits the authority of the OCC to address unsafe or unsound practices or conditions, unfair or deceptive practices, or other violations of law. 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. *Relationship to Other Legal Requirements.* Actions by a national bank or Federal savings association in connection with residential mortgage lending that are inconsistent with these Guidelines or Appendix A to this

part 30 may also constitute unsafe or unsound practices for purposes of section 8 of the Federal Deposit Insurance Act, 12 U.S.C. 1818, unfair or deceptive practices for purposes of section 5 of the FTC Act, 15 U.S.C. 45, and the OCC's Lending Rules, 12 CFR 34.3 (Lending Rules) and Real Estate Lending Standards, 12 CFR part 34, subpart D, in the case of national banks, and 12 CFR 160.100 and 160.101, in the case of Federal savings associations, or violations of the ECOA and FHA.

D. *Definitions.*

1. Except as modified in these 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 these Guidelines, the following definitions apply:

a. *Residential mortgage loan* means any loan or other extension of credit made to one or more individuals for personal, family, or household purposes secured by an owner-occupied 1–4 family residential dwelling, including a cooperative unit or mobile home.

b. *National bank or Federal savings association* means any national bank, Federal savings association, Federal branch or Federal agency of a foreign bank, and any operating subsidiary thereof that is subject to these Guidelines.

II. Standards for Residential Mortgage Lending Practices

A. *General.* A national bank's or Federal savings association's residential mortgage lending activities should reflect standards and practices consistent with and appropriate to the size and complexity of the bank or savings association and the nature and scope of its lending activities.

B. *Objectives.* A national bank's or Federal savings association's residential mortgage lending activities should reflect standards and practices that:

1. Enable the national bank or Federal savings association to effectively manage the credit, legal, compliance, reputation, and other risks associated with the bank's or savings association's consumer residential mortgage lending activities.

2. Effectively prevent the national bank or Federal savings association from becoming engaged in abusive, predatory, unfair, or deceptive practices, directly, indirectly through mortgage brokers or other intermediaries, or through purchased loans.

III. Implementation of Residential Mortgage Lending Standards

A. *Avoidance of Particular Loan Terms, Conditions, and Features.* A national bank or Federal savings association should not become involved, directly or indirectly in residential mortgage lending activities involving abusive, predatory, unfair or deceptive lending practices, including, but not limited to:

1. *Equity Stripping and Fee Packing.* Repeat refinancings where a borrower's equity is depleted as a result of financing excessive fees for the loan or ancillary products.

2. *Loan Flipping.* Repeat refinancings under circumstances where the relative terms of the new and refinanced loan and the cost of the new loan do not provide a tangible economic benefit to the borrower.

3. *Refinancing of Special Mortgages.* Refinancing of a special subsidized mortgage that contains terms favorable to the borrower with a loan that does not provide a tangible economic benefit to the borrower relative to the refinanced loan.

4. *Encouragement of Default.* Encouraging a borrower to breach a contract and default on an existing loan prior to and in connection with the consummation of a loan that refinances all or part of the existing loan.

B. *Prudent Consideration of Certain Loan Terms, Conditions and Features.* Certain loan terms, conditions and features, may, under particular circumstances, be susceptible to abusive, predatory, unfair or deceptive practices, yet may be appropriate and acceptable risk mitigation measures, consistent with safe and sound lending, and benefit customers under other circumstances. A national bank or Federal savings association should prudently consider the circumstances, including the characteristics of a targeted market and applicable consumer and safety and soundness safeguards, under which the national bank or Federal savings association will engage directly or indirectly in making residential mortgage loans with the following loan terms, conditions and features:

1. Financing single premium credit life, disability or unemployment insurance.

2. Negative amortization, involving a payment schedule in which regular periodic payments cause the principal balance to increase.

3. Balloon payments in short-term transactions.

4. Prepayment penalties that are not limited to the early years of the loan, particularly in subprime loans.

5. Interest rate increases upon default at a level not commensurate with risk mitigation.

6. Call provisions permitting the national bank or Federal savings association to accelerate payment of the loan under circumstances other than the borrower's default under the credit agreement or to mitigate the bank's or savings association's exposure to loss.

7. Absence of an appropriate assessment and documentation of the consumer's ability to repay the loan in accordance with its

terms, commensurate with the type of loan, as required by appendix A of this part.

8. Mandatory arbitration clauses or agreements, particularly if the eligibility of the loan for purchase in the secondary market is thereby impaired.

9. Pricing terms that result in the loan's being subject to the provisions of the Home Ownership and Equity Protection Act. 15 U.S.C. 1639 *et seq*.

10. Original principal balance of the loan in excess of appraised value.

11. Payment schedules that consolidate more than two periodic payments and pay them in advance from the loan proceeds.

12. Payments to home improvement contractors under a home improvement contract from the proceeds of a residential mortgage loan other than by an instrument payable to the consumer, jointly to the consumer and the contractor, or through an independent third party escrow agent.

C. *Enhanced Care to Avoid Abusive Loan Terms, Conditions, and Features in Certain Mortgages.* A national bank or Federal savings association may face heightened risks when it solicits or offers loans to consumers who are not financially sophisticated, have language barriers, or are elderly, or have limited or poor credit histories, are substantially indebted, or have other characteristics that limit their credit choices. In connection with such consumers, a national bank or Federal savings association should exercise enhanced care if it employs the residential mortgage loan terms, conditions, and features described in paragraph B of this section III, and should also apply appropriate heightened internal controls and monitoring to any line of business that does so.

D. *Avoidance of Consumer Misunderstanding.* A national bank's or Federal savings association's residential mortgage lending activities should include provision of timely, sufficient, and accurate information to a consumer concerning the terms and costs, risks, and benefits of the loan. Consumers should be provided with information sufficient to draw their attention to these key terms.

E. *Purchased and Brokered Loans.* With respect to consumer residential mortgage loans that the national bank or Federal savings association purchases, or makes through a mortgage broker or other intermediary, the national bank or Federal savings association's residential mortgage lending activities should reflect standards and practices consistent with those applied by the bank or savings association in its direct lending activities and include appropriate measures to mitigate risks, such as the following:

1. Criteria for entering into and continuing relationships with intermediaries and originators, including due diligence requirements.

2. Underwriting and appraisal requirements.

3. Standards related to total loan compensation and total compensation of intermediaries, including maximum rates, points, and other charges, and the use of overages and yield-spread premiums, structured to avoid providing an incentive to originate loans with predatory or abusive characteristics.

4. Requirements for agreements with intermediaries and originators, including with respect to risks identified in the due diligence process, compliance with appropriate national bank or Federal savings association policies, procedures and practices and with applicable law (including remedies for failure to comply), protection of the national bank or Federal savings association against risk, and termination procedures.

5. Loan documentation procedures, management information systems, quality control reviews, and other methods through which the national bank or Federal savings association will verify compliance with agreements, bank or savings association policies, and applicable laws, and otherwise retain appropriate oversight of mortgage origination functions, including loan sourcing, underwriting, and loan closings.

6. Criteria and procedures for the national bank or Federal savings association to take appropriate corrective action, including modification of loan terms and termination of the relationship with the intermediary or originator in question.

F. *Monitoring and Corrective Action.* A national bank's or Federal savings association's consumer residential mortgage lending activities should include appropriate monitoring of compliance with applicable law and the bank's or savings association's lending standards and practices, periodic monitoring and evaluation of the nature, quantity and resolution of customer complaints, and appropriate evaluation of the effectiveness of the bank's or savings association's standards and practices in accomplishing the objectives set forth in these Guidelines. The bank's or savings association's activities also should include appropriate steps for taking corrective action in response to failures to comply with applicable law and the bank's or savings association's lending standards, and for making adjustments to the bank's or savings association's activities as may be appropriate to enhance their effectiveness or to reflect changes in business practices, market conditions, or the bank's or savings association's lines of business, residential mortgage loan programs, or customer base.

[70 FR 6332, Feb. 7, 2005, as amended at 79 FR 54544, Sept. 11, 2014]

APPENDIX D TO PART 30—OCC GUIDELINES ESTABLISHING HEIGHTENED STANDARDS FOR CERTAIN LARGE INSURED NATIONAL BANKS, INSURED FEDERAL SAVINGS ASSOCIATIONS, AND INSURED FEDERAL BRANCHES

TABLE OF CONTENTS

I. INTRODUCTION

1. The OCC expects a covered bank, as that term is defined in paragraph I.E. to establish and implement a risk governance framework to manage and control the covered bank's risk-taking activities.

2. This appendix establishes minimum standards for the design and implementation of a covered bank's risk governance framework and minimum standards for the covered bank's board of directors in providing oversight to the framework's design and implementation (Guidelines). These standards are in addition to any other applicable requirements in law or regulation.

3. A covered bank may use its parent company's risk governance framework in its entirety, without modification, if the framework meets these minimum standards, the risk profiles of the parent company and the covered bank are substantially the same as set forth in paragraph I.4. of these Guidelines, and the covered bank has demonstrated through a documented assessment that its risk profile and its parent company's risk profile are substantially the same. The assessment should be conducted at least annually, in conjunction with the review and update of the risk governance framework performed by independent risk management, as set forth in paragraph II.A. of these Guidelines.

4. A parent company's and covered bank's risk profiles are substantially the same if, as reported on the covered bank's Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Reports) for the four most recent consecutive quarters, the covered bank's average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, represent 95 percent or more of the parent company's average total consolidated assets.[1] A covered bank that does not satisfy this test may submit a written analysis to the OCC for consideration and approval that demonstrates that the risk profile of the parent company and the covered bank are substantially the same based upon other factors not specified in this paragraph.

5. Subject to paragraph I.6. of these Guidelines, a covered bank should establish its own risk governance framework when the parent company's and covered bank's risk profiles are not substantially the same. The covered bank's framework should ensure that the covered bank's risk profile is easily distinguished and separate from that of its parent for risk management and supervisory reporting purposes and that the safety and soundness of the covered bank is not jeopardized by decisions made by the parent company's board of directors and management.

6. When the parent company's and covered bank's risk profiles are not substantially the same, a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company's risk governance framework when developing its own risk governance framework to the extent

[1] For a parent company, average total consolidated assets means the average of the parent company's total consolidated assets, as reported on the parent company's Form FR Y–9C to the Board of Governors of the Federal Reserve System, or equivalent regulatory report, for the four most recent consecutive quarters.

those components are consistent with the objectives of these Guidelines.

A. *Scope*

These Guidelines apply to any bank, as that term is defined in paragraph I.E. of these Guidelines, with average total consolidated assets equal to or greater than $50 billion. In addition, these Guidelines apply to any bank with average total consolidated assets less than $50 billion if that institution's parent company controls at least one covered bank. For a covered bank, average total consolidated assets means the average of the covered bank's total consolidated assets, as reported on the covered bank's Call Reports, for the four most recent consecutive quarters.

B. *Compliance Date*

1. *Initial compliance.* The date on which a covered bank should comply with the Guidelines is set forth below:

(a) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $750 billion as of November 10, 2014 should comply with these Guidelines on November 10, 2014;

(b) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $100 billion but less than $750 billion as of November 10, 2014 should comply with these Guidelines within six months from November 10, 2014;

(c) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $50 billion but less than $100 billion as of November 10, 2014 should comply with these Guidelines within 18 months from November 10, 2014;

(d) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, less than $50 billion that is a covered bank because that bank's parent company controls at least one other covered bank as of November 10, 2014 should comply with these Guidelines on the date that such other covered bank should comply; and

(e) A covered bank that does not come within the scope of these Guidelines on November 10, 2014, but subsequently becomes subject to the Guidelines because average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, are equal to or greater than $50 billion after November 10, 2014, should comply with these Guidelines within 18 months from the as-of date of the most recent Call Report used in the calculation of the average.

C. *Reservation of Authority*

1. The OCC reserves the authority to apply these Guidelines, in whole or in part, to a bank that has average total consolidated assets less than $50 billion, if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of these Guidelines;

2. The OCC reserves the authority, for each covered bank, to extend the time for compliance with these Guidelines or modify these Guidelines; or

3. The OCC reserves the authority to determine that compliance with these Guidelines should no longer be required for a covered bank. The OCC would generally make the determination under this paragraph I.C.3. if a covered bank's operations are no longer highly complex or no longer present a heightened risk. In determining whether a covered bank's operations are highly complex or present a heightened risk, the OCC will consider the following factors: Complexity of products and services, risk profile, and scope of operations.

4. When exercising the authority in this paragraph I.C., the OCC will apply notice and response procedures, when appropriate, in the same manner and to the same extent as the notice and response procedures in 12 CFR 3.404.

D. *Preservation of Existing Authority*

Neither section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1) nor these Guidelines in any way limits the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law. 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.

E. *Definitions*

1. *Bank* means any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank.

2. *Chief Audit Executive* means an individual who leads internal audit and is one level below the Chief Executive Officer in a covered bank's organizational structure.

3. *Chief Risk Executive* means an individual who leads an independent risk management unit and is one level below the Chief Executive Officer in a covered bank's organizational structure. A covered bank may have more than one Chief Risk Executive.

4. *Control.* A parent company *controls* a covered bank if it:

(a) Owns, controls, or holds with power to vote 25 percent or more of a class of voting securities of the covered bank; or

(b) Consolidates the covered bank for financial reporting purposes.

5. *Covered bank* means any bank:

(a) With average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $50 billion;

(b) With average total consolidated assets less than $50 billion if that bank's parent company controls at least one covered bank; or

(c) With average total consolidated assets less than $50 billion, if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of these Guidelines pursuant to paragraph I.C. of these Guidelines.

6. *Front Line Unit.* (a) Except as provided in paragraph (b) of this definition, *front line unit* means any organizational unit or function thereof in a covered bank that is accountable for a risk in paragraph II.B. of these Guidelines that:

(i) Engages in activities designed to generate revenue or reduce expenses for the parent company or covered bank;

(ii) Provides operational support or servicing to any organizational unit or function within the covered bank for the delivery of products or services to customers; or

(iii) Provides technology services to any organizational unit or function covered by these Guidelines.

(b) *Front line unit* does not ordinarily include an organizational unit or function thereof within a covered bank that provides legal services to the covered bank.

7. *Independent risk management* means any organizational unit within a covered bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Such units maintain independence from front line units through the following reporting structure:

(a) The board of directors or the board's risk committee reviews and approves the risk governance framework;

(b) Each Chief Risk Executive has unrestricted access to the board of directors and its committees to address risks and issues identified through independent risk management's activities;

(c) The board of directors or its risk committee approves all decisions regarding the appointment or removal of the Chief Risk Executive(s) and approves the annual compensation and salary adjustment of the Chief Risk Executive(s); and

(d) No front line unit executive oversees any independent risk management unit.

8. *Internal audit* means the organizational unit within a covered bank that is designated to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B. Internal audit maintains independence from front line units and independent risk management through the following reporting structure:

(a) The Chief Audit Executive has unrestricted access to the board's audit committee to address risks and issues identified through internal audit's activities;

(b) The audit committee reviews and approves internal audit's overall charter and audit plans;

(c) The audit committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the Chief Audit Executive;

(d) The audit committee or the Chief Executive Officer oversees the Chief Audit Executive's administrative activities; and

(e) No front line unit executive oversees internal audit.

9. *Parent company* means the top-tier legal entity in a covered bank's ownership structure.

10. *Risk appetite* means the aggregate level and types of risk the board of directors and management are willing to assume to achieve a covered bank's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements.

11. *Risk profile* means a point-in-time assessment of a covered bank's risks, aggregated within and across each relevant risk category, using methodologies consistent with the risk appetite statement described in paragraph II.E. of these Guidelines.

II. Standards for Risk Governance Framework

A. *Risk Governance Framework.* A covered bank should establish and adhere to a formal, written risk governance framework that is designed by independent risk management and approved by the board of directors or the board's risk committee. The risk governance framework should include delegations of authority from the board of directors to management committees and executive officers as well as the risk limits established for material activities. Independent risk management should review and update the risk governance framework at least annually, and as often as needed to address improvements in industry risk management practices and changes in the covered bank's risk profile caused by emerging risks, its strategic plans, or other internal and external factors.

B. *Scope of Risk Governance Framework.* The risk governance framework should cover the following risk categories that apply to the covered bank: Credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk.

C. *Roles and Responsibilities.* The risk governance framework should include well-defined risk management roles and responsibilities for front line units, independent risk

management, and internal audit.[2] The roles and responsibilities for each of these organizational units should be:

1. *Role and Responsibilities of Front Line Units.* Front line units should take responsibility and be held accountable by the Chief Executive Officer and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. In fulfilling this responsibility, each front line unit should, either alone or in conjunction with another organizational unit that has the purpose of assisting a front line unit:

(a) Assess, on an ongoing basis, the material risks associated with its activities and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs II.C.1.(b) and (c) of these Guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the unit's risk profile or other conditions;

(b) Establish and adhere to a set of written policies that include front line unit risk limits as discussed in paragraph II.F. of these Guidelines. Such policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the covered bank's risk appetite statement, concentration risk limits, and all policies established within the risk governance framework under paragraphs II.C.2.(c) and II.G. through K. of these Guidelines;

(c) Establish and adhere to procedures and processes, as necessary, to maintain compliance with the policies described in paragraph II.C.1.(b) of these Guidelines;

(d) Adhere to all applicable policies, procedures, and processes established by independent risk management;

(e) Develop, attract, and retain talent and maintain staffing levels required to carry out the unit's role and responsibilities effectively, as set forth in paragraphs II.C.1.(a) through (d) of these Guidelines;

(f) Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and

(g) Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

2. *Role and Responsibilities of Independent Risk Management.* Independent risk management should oversee the covered bank's risk-taking activities and assess risks and issues independent of front line units. In fulfilling these responsibilities, independent risk management should:

(a) Take primary responsibility and be held accountable by the Chief Executive Officer and the board of directors for designing a comprehensive written risk governance framework that meets these Guidelines and is commensurate with the size, complexity, and risk profile of the covered bank;

(b) Identify and assess, on an ongoing basis, the covered bank's material aggregate risks and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs II.C.2.(c) and (d) of these Guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the covered bank's risk profile or other conditions;

(c) Establish and adhere to enterprise policies that include concentration risk limits. Such policies should state how aggregate risks within the covered bank are effectively identified, measured, monitored, and controlled, consistent with the covered bank's risk appetite statement and all policies and processes established within the risk governance framework under paragraphs II.G. through K. of these Guidelines;

(d) Establish and adhere to procedures and processes, as necessary, to ensure compliance with the policies described in paragraph II.C.2.(c) of these Guidelines;

(e) Identify and communicate to the Chief Executive Officer and the board of directors or the board's risk committee:

(i) Material risks and significant instances where independent risk management's assessment of risk differs from that of a front line unit; and

(ii) Significant instances where a front line unit is not adhering to the risk governance framework, including instances when front line units do not meet the standards set forth in paragraph II.C.1. of these Guidelines;

(f) Identify and communicate to the board of directors or the board's risk committee:

(i) Material risks and significant instances where independent risk management's assessment of risk differs from the Chief Executive Officer; and

[2] These roles and responsibilities are in addition to any roles and responsibilities set forth in Appendices A, B, and C to Part 30. Many of the risk management practices established and maintained by a covered bank to meet these standards, including loan review and credit underwriting and administration practices, should be components of its risk governance framework, within the construct of the three distinct units identified herein. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks, *e.g.*, compliance risk management. These risk-specific programs should also be considered components of the risk governance framework, within the context of the three units described in paragraph II.C. of these Guidelines.

(ii) Significant instances where the Chief Executive Officer is not adhering to, or holding front line units accountable for adhering to, the risk governance framework;

(g) Develop, attract, and retain talent and maintain staffing levels required to carry out its role and responsibilities effectively, as set forth in paragraphs II.C.2.(a) through (f) of these Guidelines;

(h) Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and

(i) Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

3. *Role and Responsibilities of Internal Audit.* In addition to meeting the standards set forth in appendix A of part 30, internal audit should ensure that the covered bank's risk governance framework complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank. In carrying out its responsibilities, internal audit should:

(a) Maintain a complete and current inventory of all of the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan described in paragraph II.C.3.(b) of these Guidelines;

(b) Establish and adhere to an audit plan that is periodically reviewed and updated that takes into account the covered bank's risk profile, emerging risks, and issues, and establishes the frequency with which activities should be audited. The audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and independent risk management under the risk governance framework. Significant changes to the audit plan should be communicated to the board's audit committee;

(c) Report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan described in paragraph II.C.3.(b) of these Guidelines to the board's audit committee. Internal audit's reports to the audit committee should also identify the root cause of any material issues and include:

(i) A determination of whether the root cause creates an issue that has an impact on one organizational unit or multiple organizational units within the covered bank; and

(ii) A determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner;

(d) Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. The independent assessment should include a conclusion on the covered bank's compliance with the standards set forth in these Guidelines;[3]

(e) Identify and communicate to the board's audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework;

(f) Establish a quality assurance program that ensures internal audit's policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed;

(g) Develop, attract, and retain talent and maintain staffing levels required to effectively carry out its role and responsibilities, as set forth in paragraphs II.C.3.(a) through (f) of these Guidelines;

(h) Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and

(i) Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

D. *Strategic Plan.* The Chief Executive Officer should be responsible for the development of a written strategic plan with input from front line units, independent risk management, and internal audit. The board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually. The strategic plan should cover, at a minimum, a three-year period and:

1. Contain a comprehensive assessment of risks that currently have an impact on the covered bank or that could have an impact on the covered bank during the period covered by the strategic plan;

2. Articulate an overall mission statement and strategic objectives for the covered bank, and include an explanation of how the covered bank will achieve those objectives;

3. Include an explanation of how the covered bank will update, as necessary, the risk governance framework to account for changes in the covered bank's risk profile projected under the strategic plan; and

4. Be reviewed, updated, and approved, as necessary, due to changes in the covered bank's risk profile or operating environment that were not contemplated when the strategic plan was developed.

[3]The annual independent assessment of the risk governance framework may be conducted by internal audit, an external party, or internal audit in conjunction with an external party.

E. *Risk Appetite Statement.* A covered bank should have a comprehensive written statement that articulates the covered bank's risk appetite and serves as the basis for the risk governance framework. The risk appetite statement should include both qualitative components and quantitative limits. The qualitative components should describe a safe and sound risk culture and how the covered bank will assess and accept risks, including those that are difficult to quantify. Quantitative limits should incorporate sound stress testing processes, as appropriate, and address the covered bank's earnings, capital, and liquidity. The covered bank should set limits at levels that take into account appropriate capital and liquidity buffers and prompt management and the board of directors to reduce risk before the covered bank's risk profile jeopardizes the adequacy of its earnings, liquidity, and capital.[4]

F. *Concentration and Front Line Unit Risk Limits.* The risk governance framework should include concentration risk limits and, as applicable, front line unit risk limits, for the relevant risks. Concentration and front line unit risk limits should limit excessive risk taking and, when aggregated across such units, provide that these risks do not exceed the limits established in the covered bank's risk appetite statement.

G. *Risk Appetite Review, Monitoring, and Communication Processes.* The risk governance framework should require:[5]

1. Review and approval of the risk appetite statement by the board of directors or the board's risk committee at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the covered bank's business model, strategy, risk profile, or market conditions;

2. Initial communication and ongoing reinforcement of the covered bank's risk appetite statement throughout the covered bank in a manner that causes all employees to align their risk-taking decisions with applicable aspects of the risk appetite statement;

3. Monitoring by independent risk management of the covered bank's risk profile relative to its risk appetite and compliance with concentration risk limits and reporting on such monitoring to the board of directors or the board's risk committee at least quarterly;

4. Monitoring by front line units of compliance with their respective risk limits and reporting to independent risk management at least quarterly; and

5. When necessary due to the level and type of risk, monitoring by independent risk management of front line units' compliance with front line unit risk limits, ongoing communication with front line units regarding adherence to these limits, and reporting of any concerns to the Chief Executive Officer and the board of directors or the board's risk committee, as set forth in paragraphs II.C.2.(e) and (f) of these Guidelines, all at least quarterly.

H. *Processes Governing Risk Limit Breaches.* A covered bank should establish and adhere to processes that require front line units and independent risk management, in conjunction with their respective responsibilities, to:

1. Identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits;

2. Distinguish breaches based on the severity of their impact on the covered bank;

3. Establish protocols for when and how to inform the board of directors, front line unit management, independent risk management, internal audit, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the covered bank;

4. Include in the protocols established in paragraph II.H.3. of these Guidelines the requirement to provide a written description of how a breach will be, or has been, resolved; and

5. Establish accountability for reporting and resolving breaches that include consequences for risk limit breaches that take into account the magnitude, frequency, and recurrence of breaches.

I. *Concentration Risk Management.* The risk governance framework should include policies and supporting processes appropriate for the covered bank's size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the covered bank's concentrations of risk.

J. *Risk Data Aggregation and Reporting.* The risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for:

---

[4] Where possible, covered banks should establish aggregate risk appetite limits that can be disaggregated and applied at the front line unit level. However, where this is not possible, covered banks should establish limits that reasonably reflect the aggregate level of risk that the board of directors and executive management are willing to accept.

[5] With regard to paragraphs 3., 4., and 5. in this paragraph II.G., the frequency of monitoring and reporting should be performed more often, as necessary, based on the size and volatility of risks and any material change in the covered bank's business model, strategy, risk profile, or market conditions.

1. The design, implementation, and maintenance of a data architecture and information technology infrastructure that support the covered bank's risk aggregation and reporting needs during normal times and during times of stress;

2. The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC; and

3. The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

K. *Relationship of Risk Appetite Statement, Concentration Risk Limits, and Front Line Unit Risk Limits to Other Processes.* A covered bank's front line units and independent risk management should incorporate at a minimum the risk appetite statement, concentration risk limits, and front line unit risk limits into the following:

1. Strategic and annual operating plans;

2. Capital stress testing and planning processes;

3. Liquidity stress testing and planning processes;

4. Product and service risk management processes, including those for approving new and modified products and services;

5. Decisions regarding acquisitions and divestitures; and

6. Compensation and performance management programs.

L. *Talent Management Processes.* A covered bank should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. The board of directors or an appropriate committee of the board should:

1. Appoint a Chief Executive Officer and appoint or approve the appointment of a Chief Audit Executive and one or more Chief Risk Executives with the skills and abilities to carry out their roles and responsibilities within the risk governance framework;

2. Review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the individuals described in paragraph II.L.1. of these Guidelines, their direct reports, and other potential successors; and

3. Require management to assign individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program's effectiveness.

M. *Compensation and Performance Management Programs.* A covered bank should establish and adhere to compensation and performance management programs that comply with any applicable statute or regulation and are appropriate to:

1. Ensure the Chief Executive Officer, front line units, independent risk management, and internal audit implement and adhere to an effective risk governance framework;

2. Ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit, as well as the timeliness of corrective action to resolve such issues and concerns;

3. Attract and retain the talent needed to design, implement, and maintain an effective risk governance framework; and

4. Prohibit any incentive-based payment arrangement, or any feature of any such arrangement, that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

III. Standards for Board of Directors

A. *Require an Effective Risk Governance Framework.* Each member of a covered bank's board of directors should oversee the covered bank's compliance with safe and sound banking practices. The board of directors should also require management to establish and implement an effective risk governance framework that meets the minimum standards described in these Guidelines. The board of directors or the board's risk committee should approve any significant changes to the risk governance framework and monitor compliance with such framework.

B. *Provide Active Oversight of Management.* A covered bank's board of directors should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board of directors may rely on risk assessments and reports prepared by independent risk management and internal audit to support the board's ability to question, challenge, and when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the covered bank.

C. *Exercise Independent Judgment.* When providing active oversight under paragraph III.B. of these Guidelines, each member of the board of directors should exercise sound, independent judgment.

D. *Include Independent Directors.* To promote effective, independent oversight of the covered bank's management, at least two members of the board of directors:[6]

[6] This provision does not supersede other regulatory requirements regarding the composition of the Board that apply to Federal

Continued

1. Should not be an officer or employee of the parent company or covered bank and has not been an officer or employee of the parent company or covered bank during the previous three years;

2. Should not be a member of the immediate family, as defined in §225.41(b)(3) of the Board of Governors of the Federal Reserve System's Regulation Y (12 CFR 225.41(b)(3)), of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, as defined in §215.2(e)(1) of Regulation O (12 CFR 215.2(e)(1)); and

3. Should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.

E. *Provide Ongoing Training to All Directors.* The board of directors should establish and adhere to a formal, ongoing training program for all directors. This program should consider the directors' knowledge and experience and the covered bank's risk profile. The program should include, as appropriate, training on:

1. Complex products, services, lines of business, and risks that have a significant impact on the covered bank;

2. Laws, regulations, and supervisory requirements applicable to the covered bank; and

3. Other topics identified by the board of directors.

F. *Self-Assessments.* A covered bank's board of directors should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards in section III of these Guidelines.

[79 FR 54545, Sept. 11, 2014]

PART 31—EXTENSIONS OF CREDIT TO INSIDERS AND TRANSACTIONS WITH AFFILIATES

Sec.

AUTHORITY: 12 U.S.C. 93a, 375a(4), 375b(3), and 1817(k).

SOURCE: 61 FR 54536, Oct. 21, 1996, unless otherwise noted.

§31.1 Authority.

This part is issued by the Comptroller of the Currency pursuant to 12 U.S.C. 93a, 375a(4), 375b(3), 1817(k) and 1817(k), as amended.

[61 FR 54536, Oct. 21, 1996, as amended at 73 FR 22251, Apr. 24, 2008]

§31.2 Insider lending restrictions and reporting requirements.

(a) *General rule.* A national bank and its insiders shall comply with the provisions contained in 12 CFR part 215.

(b) *Enforcement.* The Comptroller of the Currency administers and enforces insider lending standards and reporting requirements as they apply to national banks and their insiders.

APPENDIX A TO PART 31—INTERPRETATIONS: DEPOSITS BETWEEN AFFILIATED BANKS

a. *General rule.* A deposit made by a bank in an affiliated bank is treated as a loan or extension of credit to the affiliate bank under 12 U.S.C. 371c, as this statute is implemented by the Federal Reserve Board's Regulation W, 12 CFR part 223. Thus, unless an exemption from Regulation W is available, these deposits must be secured in accordance with 12 CFR 223.14. However, a national bank may not pledge assets to secure private deposits unless otherwise permitted by law (*see, e.g.*, 12 U.S.C. 90 (permitting collateralization of deposits of public funds); 12 U.S.C. 92a (trust funds); and 25 U.S.C. 156 and 162a (Native American funds)). Thus, unless one of the exceptions to 12 CFR part 223 noted in paragraph b. of this interpretation applies, unless another exception applies that enables a bank to meet the collateral requirements of §223.14, or unless a party other than the bank in which the deposit is made can legally offer and does post the required collateral, a national bank may not:

1. Make a deposit in an affiliated national bank;

2. Make a deposit in an affiliated State-chartered bank unless the affiliated State-chartered bank can legally offer collateral for the deposit in conformance with applicable State law and 12 CFR 223.14; or

3. Receive deposits from an affiliated bank.

b. *Exceptions.* The restrictions of 12 CFR part 223 (other than 12 CFR 223.13, which requires affiliate transactions to be consistent with safe and sound banking practices) do not apply to deposits:

1. Made in an affiliated depository institution or affiliated foreign bank provided that the deposit represents an ongoing, working balance maintained in the ordinary course of

---

savings associations. These institutions must continue to comply with such other requirements.