Proposed Rules

Federal Register
Vol. 80, No. 20
Friday, January 30, 2015

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF ENERGY

10 CFR Part 430

[Docket No. EERE–2013–BT–STD–0051]

RIN 1904–AD09

Energy Efficiency Program for Consumer Products: Energy Conservation Standards for General Service Lamps: Preliminary Technical Support Document

AGENCY: Office of Energy Efficiency and Renewable Energy, Department of Energy.

ACTION: Extension of public comment period.

SUMMARY: This document announces an extension of the time period for submitting comments, data and information on the preliminary technical support document (TSD) for general service lamps (GSLs) energy conservation standards published on December 11, 2014. The comment period is extended to February 23, 2015.

DATES: The comment period for the preliminary TSD for GSLs published on December 11, 2014 (79 FR 73503) is extended to February 23, 2015.

ADDRESSES: Interested persons may submit comments, identified by docket number EERE–2013–BT–STD–0051 and/or Regulation Identification Number (RIN) 1904–AD09, by any of the following methods:

- *Federal eRulemaking Portal: www.regulations.gov*. Follow the instructions for submitting comments.
- *Email: GSL2013STD0051@ee.doe.gov*. Include the docket number EERE–2013–BT–STD–0051 and/or RIN 1904–AD09 in the subject line of the message.
- *Mail:* Ms. Brenda Edwards, U.S. Department of Energy, Building Technologies Program, Mailstop EE–5B, 1000 Independence Avenue SW., Washington, DC 20585–0121. If possible, please submit all items on a compact disc (CD), in which case it is not necessary to include printed copies. [Please note that comments and CDs sent by mail are often delayed and may be damaged by mail screening processes.]
- *Hand Delivery/Courier:* Ms. Brenda Edwards, U.S. Department of Energy, Building Technologies Program, 950 L'Enfant Plaza SW., Suite 600, Washington, DC 20024. Telephone (202) 586–2945. If possible, please submit all items on CD, in which case it is not necessary to include printed copies.

Docket: The docket is available for review at *www.regulations.gov,* including **Federal Register** notices, framework documents, public meeting attendee lists and transcripts, comments, and other supporting documents/materials. All documents in the docket are listed in the *www.regulations.gov* index. However, not all documents listed in the index may be publicly available, such as information that is exempt from public disclosure.

The rulemaking Web page can be found at: *http://www1.eere.energy.gov/buildings/appliance_standards/rulemaking.aspx/ruleid/83*. This Web page contains a link to the docket for this notice on the regulation.gov site. The *www.regulations.gov* Web page contains instructions on how to access all documents in the docket, including public comments.

FOR FURTHER INFORMATION CONTACT: Ms. Lucy deButts, U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, Building Technologies, EE–5B, 1000 Independence Avenue SW., Washington, DC 20585–0121. Telephone: (202)-287–1604. Email: *GSL@ee.doe.gov*.

In the Office of the General Counsel, contact Ms. Celia Sher, U.S. Department of Energy, Office of the General Counsel, GC–33, 1000 Independence Avenue SW., Washington, DC 20585–0121. Telephone: (202) 287–6122. Email: *Celia.Sher@hq.doe.gov*.

SUPPLEMENTARY INFORMATION: On December 11, 2014, the U.S. Department of Energy (DOE) published a notice of public meeting and availability of the preliminary TSD in the **Federal Register** to make available and invite comments on the preliminary analysis for establishing energy conservation standards for GSLs. 79 FR 73503. The notice provided for the written submission of comments by February 9, 2015, and oral comments were also accepted at a public meeting held on January 20, 2015. The National Electrical Manufacturers Association requested an extension of the public comment period to ensure adequate time to consider the preliminary technical support document and public meeting presentation, and to prepare and submit comments accordingly.

DOE has determined that an extension of the public comment period is appropriate to allow interested parties additional time to submit comments for DOE's consideration. Thus, DOE is extending the comment period by 14 days. DOE will consider any comments received by midnight of February 23, 2015 to be timely submitted.

Issued in Washington, DC, on January 26, 2015.

Kathleen B. Hogan,

Deputy Assistant Secretary for Energy Efficiency, Energy Efficiency and Renewable Energy.

[FR Doc. 2015–01779 Filed 1–29–15; 8:45 am]

BILLING CODE 6450–01–P

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Parts 308, 364 and 391

RIN 3064–AE28

Transferred OTS Regulations Regarding Safety and Soundness Guidelines and Compliance Procedures and Amendments

AGENCY: Federal Deposit Insurance Corporation.

ACTION: Notice of proposed rulemaking.

SUMMARY: In this notice of proposed rulemaking, the Federal Deposit Insurance Corporation (FDIC) proposes to rescind and remove from the Code of Federal Regulations 12 CFR part 391, subpart B, entitled ''Safety and Soundness Guidelines and Compliance Procedures'' and Appendix A and B to part 391, subpart B and supplement A to appendix B. With few exceptions addressed below, the requirements for state savings associations in part 391, subpart B, are substantively similar to those in the FDIC's 12 CFR part 308, subpart R, and in the FDIC's 12 CFR part 364.

Upon the completion of these proposed changes, the ''Standards for Safety and Soundness'' for all insured

depository institutions for which the FDIC has been designated the appropriate Federal banking agency will be found at part 364 and the ''Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies'' for all insured depository institutions for which the FDIC has been designated the appropriate Federal banking agency will be found at part 308, subpart R.

DATES: Comments must be received on or before March 31, 2015.

ADDRESSES: You may submit comments by any of the following methods:

- *FDIC Web site: http://www.fdic.gov/regulations/laws/federal/.* Follow instructions for submitting comments on the agency Web site.
- *FDIC Email: Comments@fdic.gov.* Include RIN 3064–AE28 on the subject line of the message.
- *FDIC Mail:* Robert E. Feldman, Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street NW., Washington, DC 20429.
- *Hand Delivery to FDIC:* Comments may be hand-delivered to the guard station at the rear of the 550 17th Street Building (located on F Street) on business days between 7 a.m. and 5 p.m.

Please include your name, affiliation, address, email address, and telephone number(s) in your comment. Where appropriate, comments should include a short Executive Summary consisting of no more than five single-spaced pages. All statements received, including attachments and other supporting materials, are part of the public record and are subject to public disclosure. You should submit only information that you wish to make publicly available.

Please note: All comments received will be posted generally without change to *http://www.fdic.gov/regulations/laws/federal/,* including any personal information provided. Paper copies of public comments may be requested from the Public Information Center by telephone at 1–877–275–3342 or 1–703–562–2200.

FOR FURTHER INFORMATION CONTACT: Rebecca M. Parks, Review Examiner, Division of Risk Management Supervision (202) 898–3912; Jann L. Harley, Senior Attorney, Legal Division (312) 382–6535; and Michael P. Condon, Counsel, Legal Division (202) 898–6536.

SUPPLEMENTARY INFORMATION:

I. Background

The Dodd-Frank Act

The Dodd-Frank Act provided for a substantial reorganization of the regulation of State and Federal savings associations and their holding companies. Beginning July 21, 2011, the transfer date established by section 311 of the Dodd-Frank Act, codified at 12 U.S.C. 5411, the powers, duties, and functions formerly performed by the OTS were divided among the FDIC, as to State savings associations, the Office of the Comptroller of the Currency (''OCC''), as to Federal savings associations, and the Board of Governors of the Federal Reserve System (''FRB''), as to savings and loan holding companies. Section 316(b) of the Dodd-Frank Act, codified at 12 U.S.C. 5414(b), provides the manner of treatment for all orders, resolutions, determinations, regulations, and advisory materials that had been issued, made, prescribed, or allowed to become effective by the OTS. The section provides that if such materials were in effect on the day before the transfer date, they continue in effect and are enforceable by or against the appropriate successor agency until they are modified, terminated, set aside, or superseded in accordance with applicable law by such successor agency, by any court of competent jurisdiction, or by operation of law.

Section 316(c) of the Dodd-Frank Act, codified at 12 U.S.C. 5414(c), further directed the FDIC and the OCC to consult with one another and to publish a list of the continued OTS regulations which would be enforced by the FDIC and the OCC, respectively. On June 14, 2011, the FDIC's Board of Directors approved a ''List of OTS Regulations to be Enforced by the OCC and the FDIC Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act.'' This list was published by the FDIC and the OCC as a Joint Notice in the **Federal Register** on July 6, 2011.[1]

Although section 312(b)(2)(B)(i)(II) of the Dodd-Frank Act, codified at 12 U.S.C. 5412(b)(2)(B)(i)(II), granted the OCC rulemaking authority relating to both State and Federal savings associations, nothing in the Dodd-Frank Act affected the FDIC's existing authority to issue regulations under the FDI Act and other laws as the ''appropriate Federal banking agency'' or under similar statutory terminology. Section 312(c) of the Dodd-Frank Act amended the definition of ''appropriate Federal banking agency'' contained in Section 3(q) of the FDI Act, 12 U.S.C. 1813(q), to add State savings associations to the list of entities for which the FDIC is designated as the ''appropriate Federal banking agency.'' As a result, when the FDIC acts as the designated ''appropriate Federal banking agency'' (or under similar terminology) for State savings associations, as it does here, the FDIC is authorized to issue, modify, and rescind regulations involving such associations, as well as for State nonmember banks and insured branches of foreign banks.

As noted, on June 14, 2011, operating pursuant to this authority, the FDIC's Board of Directors reissued and redesignated certain transferring regulations of the former OTS. These transferred OTS regulations were published as new FDIC regulations in the **Federal Register** on August 5, 2011.[2] When it republished the transferred OTS regulations as new FDIC regulations, the FDIC specifically noted that its staff would evaluate the transferred OTS rules and might later recommend incorporating the transferred OTS regulations into other FDIC rules, amending them, or rescinding them, as appropriate.

One of the OTS's rules transferred to the FDIC governs safety and soundness guidelines, the submission and review of safety and soundness compliance plans, and the issuance of orders to correct safety and soundness deficiencies. The OTS's rule, formerly found at 12 CFR part 570, was transferred to the FDIC with only nomenclature changes and is now found in the FDIC's rules at part 391, subpart B, entitled ''Safety and Soundness Guidelines and Compliance Procedures.'' The ''Interagency Guidelines Establishing Standards for Safety and Soundness'' were found at appendix A to part 391, subpart B, the ''Interagency Guidelines Establishing Information Security Standards'' were found at appendix B to part 391, subpart B, and the ''Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice'' were found at the supplement to appendix B to part 391, subpart B. Before the transfer of the OTS rules and continuing today, the FDIC's rules contained part 364, entitled ''Standards for Safety and Soundness,'' a rule establishing safety and soundness standards for State nonmember insured banks and to State-licensed insured branches of foreign banks, that are subject to section 39 of the FDI Act, 12 U.S.C. 1831p–1. Part 364 also established safety and soundness standards relating to information security for State nonmember insured banks, insured State licensed branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisors) as set out in appendix B to part 364, the ''Interagency Guidelines Establishing Information Security

[1] 76 FR 39247 (July 6, 2011).

[2] 76 FR 47652 (Aug. 5, 2011).

Standards'' and supplement A to appendix B to part 364, the ''Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.'' Additionally, before the transfer of the OTS rules and continuing today, the FDIC's rules contained part 308, subpart R, entitled ''Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies.''

After careful review and comparison of part 391, subpart B and part 308, subpart R, and part 364 and its accompanying appendices and supplement to appendices, the FDIC proposes to rescind subpart B of part 391 because, as discussed below, it is substantively redundant to existing part 308, subpart R, and part 364 and the accompanying appendices A and B and supplement A to appendix B.

Furthermore, to clarify that part 308, subpart R, and part 364 and its accompanying appendices A and B and supplement A to appendix B, apply to all insured depository institutions for which the FDIC has been designated the appropriate Federal banking agency, the FDIC proposes to amend part 308, subpart R, and part 364 and to reissue the appendices and supplement A to appendix B to part 364 to add ''State savings associations'' within the list of institutions to which the rules and the appendices apply.

FDIC's Existing 12 CFR Part 308, Subpart R

Section 132 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), Public Law 102–242, added Section 39 to the FDI Act (12 U.S.C. 21 1831p–1), which required each Federal banking agency to establish by regulation certain safety and soundness standards for the insured depository institutions for which it was the primary Federal regulator. Section 39 of the FDI Act was further amended on September 23, 1994 by section 318 of the Riegle Community Development and Regulatory Improvement Act of 1994, Public Law 103–325. In response to Section 39 of the FDI Act, the FDIC adopted subpart R of part 308 in 1995 to address the submission and review of safety and soundness compliance plans and issuance of orders to correct safety and soundness deficiencies.

FDIC's Existing 12 CFR Part 364 and Appendices A and B and Supplement A to Appendix B

Section 132 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), Public Law 102–242, added Section 39 to the FDI Act (12 U.S.C. 21 1831p–1), which required each Federal banking agency to establish by regulation certain safety and soundness standards for the insured depository institutions for which it was the primary Federal regulator. Section 39 of the FDI Act was further amended on September 23, 1994 by section 318 of the Riegle Community Development and Regulatory Improvement Act of 1994, Public Law 103–325. In response to Section 39 of the FDI Act, the FDIC adopted part 364 in 1995 and appendix A to part 364, the ''Interagency Guidelines Establishing Standards for Safety and Soundness,'' in 1995. The FDIC adopted appendix B to part 364, the ''Interagency Guidelines Establishing Information Security Standards,'' in 1998. The FDIC adopted supplement A to appendix B to part 364, the ''Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,'' in 2005.

Former OTS's 12 CFR Part 570 (transferred to FDIC's Part 391, Subpart B)

In 1995, the OTS adopted 12 CFR part 570 as a final rule governing safety and soundness guidelines and compliance procedures for State savings associations. The OTS adopted appendix A to part 570, the ''Interagency Guidelines Establishing Standards for Safety and Soundness,'' in 1995, adopted appendix B to part 570, the ''Interagency Guidelines Establishing Information Security Standards,'' in 1998, and adopted the supplement to appendix B, the ''Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,'' in 2005.

Despite the differences addressed above and minor technical nuances, the OTS's rule was otherwise substantively similar to the FDIC's rules governing safety and soundness guidelines and compliance procedures found in part 308, subpart R, and part 364 and its accompanying appendices. After careful comparison of the OTS part 570 (which existed prior to the transfer of the OTS rules to part 391) with the FDIC's part 308, subpart R, and the FDIC's part 364, the FDIC has concluded that the transferred OTS rules found at part 391, subpart B, and the accompanying guidelines found in appendices A and B and the supplement to appendix B, are substantively redundant. Therefore, based on the above, the FDIC proposes to rescind and remove from the Code of Federal Regulations the rules located at part 391, subpart B.

II. The Proposal

Regarding the functions of the former OTS that were transferred to the FDIC, Section 316(b)(3) of the Dodd-Frank Act, 12 U.S.C. 5414(b)(3), in pertinent part, provides that the former OTS's regulations will be enforceable by the FDIC until they are modified, terminated, set aside, or superseded in accordance with applicable law. After reviewing the rules and accompanying appendices currently found in part 391, subpart B, the FDIC, as the appropriate Federal banking agency for State savings associations, proposes to rescind part 391, subpart B in its entirety. The FDIC also proposes to amend part 364 and appendix A and B and supplement A to appendix B to include State savings associations within the scope of the regulation and guidelines. The FDIC also proposes to amend part 308, subpart R to apply to State savings associations. If the proposal is finalized, the safety and soundness guidelines in part 364 and its accompanying appendices and supplement to appendices would apply to all FDIC-supervised institutions, and the procedures found in part 308, subpart R, for the submission and review of safety and soundness compliance plans and issuance of orders to correct safety and soundness deficiencies would also apply to all FDIC-supervised institutions. Part 391, subpart B would be removed because it is redundant of the rules found in part 364 and part 308, subpart R. Rescinding part 391, subpart B, will serve to streamline the FDIC's rules and eliminate unnecessary regulations.

III. Request for Comments

The FDIC invites comments on all aspects of this proposed rulemaking, and specifically requests comments on the following:

(1.) Are the provisions of part 308, subpart R, sufficient to establish effective procedures for the submission and review of safety and soundness compliance plans and issuance of orders to correct safety and soundness deficiencies would also apply to all FDIC-supervised institutions?

(2.) Are the provisions of the proposed part 364 and the accompanying appendices and supplement to appendices sufficient to provide consistent and effective safety and soundness guidance and information security standards? Please substantiate your answer.

(3.) What impacts, positive or negative, can you foresee in the FDIC's proposal to rescind part 391, subpart B?

Written comments must be received by the FDIC no later than March 31, 2015.

IV. Regulatory Analysis and Procedure

A. The Paperwork Reduction Act

In accordance with the requirements of the Paperwork Reduction Act (''PRA'') of 1995 (44 U.S.C. 3501–3521), the FDIC may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (''OMB'') control number.

The Proposed Rule would rescind and remove part 391, subpart B, from the FDIC regulations. This rule was transferred with only nominal changes to the FDIC from the OTS when the OTS was abolished by Title III of the Dodd-Frank Act. Part 391, subpart B, is largely redundant of the FDIC's existing part 364 regarding standards for safety and soundness and subpart R of the FDIC's existing part 308 regarding the submission and review of safety and soundness compliance plans and issuance of orders to correct safety and soundness deficiencies.

The Proposed Rule would amend parts 364 and subpart R of Part 308 to include State savings associations within the scope of those regulations. This measure is to clarify that State savings associations, as well as State nonmember insured banks and foreign banks having insured branches, are all subject to part 364 and the provisions of subpart R of part 308. Thus, these provisions of the Proposed Rule will neither create any new paperwork information collections nor impact current burden estimates. Based on the above, no information collection request has been submitted to the OMB for review.

B. The Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA), requires that, in connection with a notice of proposed rulemaking, an agency prepare and make available for public comment an initial regulatory flexibility analysis that describes the impact of the proposed rule on small entities (defined in regulations promulgated by the Small Business Administration to include banking organizations with total assets of less than or equal to $550 million).[3] However, a regulatory flexibility analysis is not required if the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities, and publishes its certification and a short explanatory statement in the **Federal Register** together with the rule. For the reasons provided below, the FDIC certifies that the Proposed Rule, if adopted in final form, would not have a significant economic impact on a substantial number of small entities. Accordingly, a regulatory flexibility analysis is not required.

As discussed in this notice of proposed rulemaking, part 391, subpart B was transferred from OTS's part 570 which established safety and soundness guidelines and the process for requesting compliance plans and issuing orders to correct deficiencies. OTS's part 570 had been in effect since 1995, and all state savings associations were required to comply with it. Because it is redundant of existing part 364 of the FDIC's rules and subpart R of part 308 of the FDIC's rules, the FDIC proposes rescinding and removing part 391, subpart B. As a result, all FDIC-supervised institutions, including State savings associations, would be required to comply with part 364 and part 308, subpart R. Because all State savings associations have been required to comply with substantially similar safety and soundness guidelines and have been subject to substantially similar procedures for the filing of safety and soundness compliance plans and orders to correct deficiencies since 1995, today's Proposal would have no significant economic impact on any State savings association.

C. Plain Language

Section 722 of the GLB Act, codified at 12 U.S.C. 4809, requires each Federal banking agency to use plain language in all of its proposed and final rules published after January 1, 2000. The FDIC invites comments on whether the Proposed Rule is clearly stated and effectively organized, and how the FDIC might make it easier to understand. For example:

- Has the FDIC organized the material to suit your needs? If not, how could it present the rule more clearly?
- Have we clearly stated the requirements of the rule? If not, how could the rule be more clearly stated?
- Does the rule contain technical jargon that is not clear? If so, which language requires clarification?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the regulation easier to understand? If so, what changes would make the regulation easier to understand?
- What else could we do to make the regulation easier to understand?

D. The Economic Growth and Regulatory Paperwork Reduction Act

Under Section 2222 of the Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA), the FDIC is required to review all of its regulations, at least once every 10 years, in order to identify any outdated or otherwise unnecessary regulations imposed on insured institutions.[4] The FDIC completed the last comprehensive review of its regulations under EGRPRA in 2006 and is commencing the next decennial review. The action taken on this rule will be included as part of the EGRPRA review that is currently under way. As part of that review, the FDIC invites comments concerning whether the Proposed Rule would impose any outdated or unnecessary regulatory requirements on insured depository institutions. If you provide such comments, please be specific and provide alternatives whenever appropriate.

List of Subjects

12 CFR part 308

Banks, banking, Safety and soundness compliance plans, Savings associations.

12 CFR part 364

Banks, banking, Safety and soundness guidelines.

12 CFR part 391

Safety and soundness guidelines.

Authority and Issuance

For the reasons stated in the preamble, the Board of Directors of the Federal Deposit Insurance Corporation proposes to amend parts 308, 364, and 391 of title 12 of the Code of Federal Regulations as follows:

PART 308—RULES OF PRACTICE AND PROCEDURE

■ 1. The authority citation for part 308 continues to read as follows:

Authority: 5 U.S.C. 504, 554–557; 12 U.S.C. 93(b), 164, 505, 1815(e), 1817, 1818, 1820, 1828, 1829, 1829b, 1831i, 1831m(g)(4), 1831o, 1831p–1, 1832(c), 1884(b), 1972, 3102, 3108(a), 3349, 3909, 4717, 15 U.S.C. 78(h) and (i), 78o–4(c), 78o–5, 78q–1, 78s, 78u, 78u–2, 78u–3, and 78w, 6801(b), 6805(b)(1); 28 U.S.C. 2461 note; 31 U.S.C. 330, 5321; 42 U.S.C. 4012a; Sec. 3100(s), Pub. L. 104–134, 110 Stat. 1321–358; and Pub. L. 109–351.

■ 2. Revise subpart R of part 308 to read as follows:

[3] 5 U.S.C. 601 *et seq.*

[4] Public Law 104–208 (Sept. 30, 1996).

Subpart R—Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders To Correct Safety and Soundness Deficiencies

§ 308.300 Scope.

The rules and procedures set forth in this subpart apply to insured state nonmember banks, to state-licensed insured branches of foreign banks, that are subject to the provisions of section 39 of the Federal Deposit Insurance Act (section 39) (12 U.S.C. 1831p–1), and to state savings associations (in aggregate, bank or banks and state savings association or state savings associations).

§ 308.301 Purpose.

Section 39 of the FDI Act requires the FDIC to establish safety and soundness standards. Pursuant to section 39, a bank or savings association may be required to submit a compliance plan if it is not in compliance with a safety and soundness standard established by guideline under section 39(a) or (b). An enforceable order under section 8 of the FDI Act may be issued if, after being notified that it is in violation of a safety and soundness standard established under section 39, the bank or savings association fails to submit an acceptable compliance plan or fails in any material respect to implement an accepted plan. This subpart establishes procedures for requiring submission of a compliance plan and issuing an enforceable order pursuant to section 39.

§ 308.302 Determination and notification of failure to meet a safety and soundness standard and request for compliance plan.

(a) *Determination.* The FDIC may, based upon an examination, inspection or any other information that becomes available to the FDIC, determine that a bank or state savings association has failed to satisfy the safety and soundness standards set out in part 364 of this chapter and in the Interagency Guidelines Establishing Standards for Safety and Soundness in appendix A and the Interagency Guidelines Establishing Information Security Standards in appendix B to part 364 of this chapter.

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

§ 308.303 Filing of safety and soundness compliance plan.

(a) *Schedule for filing compliance plan*—(1) *In general.* A bank or state savings association shall file a written safety and soundness compliance plan with the FDIC within 30 days of receiving a request for a compliance plan pursuant to § 308.302(b), unless the FDIC notifies the bank or state savings association in writing that the plan is to be filed within a different period.

(2) *Other plans.* If a bank or state 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, a formal or informal agreement, or a response to a report of examination or report of inspection, it may, with the permission of the FDIC, submit a compliance plan under this section as part of that plan, order, agreement, or response, subject to the deadline provided in paragraph (a)(1) of this section.

(b) *Contents of plan.* The compliance plan shall include a description of the steps the bank or state 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 subpart, the FDIC shall provide written notice to the bank or state savings association of whether the plan has been approved or seek additional information from the bank or state savings association regarding the plan. The FDIC 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 bank or state savings association fails to submit an acceptable plan within the time specified by the FDIC or fails in any material respect to implement a compliance plan, then the FDIC shall, by order, require the bank or state 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 FDIC may be required to take certain actions if the bank or state savings association commenced operations or experienced a change in control within the previous 24-month period, or the bank or state 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 bank or state 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 bank or state savings association that has filed an approved compliance plan may, after prior written notice to and approval by the FDIC, amend the plan to reflect a change in circumstance. Until such time as a proposed amendment has been approved, the bank or state savings association shall implement the compliance plan as previously approved.

§ 308.304 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 FDIC shall provide a bank or state savings association prior written notice of the FDIC's intention to issue an order requiring the bank or state 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 bank or state savings association shall have such time to respond to a proposed order as provided by the FDIC under paragraph (c) of this section.

(2) *Immediate issuance of final order.* If the FDIC finds it necessary in order to carry out the purposes of section 39 of the FDI Act, the FDIC may, without providing the notice prescribed in paragraph (a)(1) of this section, issue an order requiring a bank or state 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 bank or state savings association that is subject to such an immediately effective order may submit a written appeal of the order to the FDIC. Such an appeal

must be received by the FDIC within 14 calendar days of the issuance of the order, unless the FDIC permits a longer period. The FDIC shall consider any such appeal, if filed in a timely matter, within 60 days of receiving the appeal. During such period of review, the order shall remain in effect unless the FDIC, in its sole discretion, stays the effectiveness of the order.

(b) *Contents 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 bank or state savings association;

(2) A description of any restrictions, prohibitions, or affirmative actions that the FDIC 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 bank or state savings association subject to the order may file with the FDIC a written response to the notice.

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

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

(i) An explanation why the action proposed by the FDIC 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 bank or state savings association regarding the proposed order.

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

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

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

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

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

§ 308.305 Enforcement of orders.

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

(b) *Failure to comply with order.* Pursuant to section 8(i)(2)(A) of the FDI Act, the FDIC may assess a civil money penalty against any bank or state 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 FDIC may seek enforcement of the provisions of section 39 or this part through any other judicial or administrative proceeding authorized by law.

■ 3. Revise part 364 to read as follows:

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

Sec.

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

§ 364.100 Purpose.

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

§ 364.101 Standards for safety and soundness.

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

(b) *Interagency Guidelines Establishing Information Security Standards.* The Interagency Guidelines Establishing Information Security Standards prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1), and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801, 6805(b)), and with respect to the proper disposal of consumer information requirements pursuant to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w), as set forth in appendix B to this part, apply to all insured state nonmember banks, insured state licensed branches of foreign banks, any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), and to state savings associations. The interagency regulations and guidelines on identity theft detection, prevention, and mitigation prescribed pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. 1681m(e), are set forth in §§ 334.90, 334.91, and Appendix J of part 334.

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

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 guidelines for all insured depository institutions. Under section 39, the agencies must establish three types of standards: (1) Operational and managerial standards; (2) compensation standards; and (3) such standards relating to asset quality, earnings, and stock valuation as they determine to be appropriate.

ii. Section 39(a) requires the agencies to establish operational and managerial standards relating to: (1) Internal controls, information systems and internal audit systems, in accordance with section 36 of the FDI Act (12 U.S.C. 1831m); (2) loan documentation; (3) credit underwriting; (4) interest rate exposure; (5) asset growth; and (6) compensation, fees, and benefits, in accordance with subsection (c) of section 39. Section 39(b) requires the agencies to establish standards relating to asset quality, earnings, and stock valuation that the agencies determine to be appropriate.

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

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

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

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

A. Preservation of Existing Authority

Neither section 39 nor these Guidelines in any way limits the authority of the agencies to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. Action under section 39 and these Guidelines may be taken independently of, in conjunction with, or in addition to any other enforcement action available to the agencies. Nothing in these Guidelines limits the authority of the FDIC pursuant to section 38(i)(2)(F) of the FDI Act (12 U.S.C. 1831(o)) and Part 325 of Title 12 of the Code of Federal Regulations.

B. Definitions

1. *In general.* For purposes of these Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in sections 3 and 39 of the FDI Act (12 U.S.C. 1813 and 1831p–1).

2. *Board of directors,* in the case of a state-licensed insured branch of a foreign bank and in the case of a federal branch of a foreign bank, means the managing official in charge of the insured foreign branch.

3. *Compensation* means all direct and indirect payments or benefits, both cash and non-cash, granted to or for the benefit of any executive officer, employee, director, or principal shareholder, including but not limited to payments or benefits derived from an employment contract, compensation or benefit agreement, fee arrangement, perquisite, stock option plan, postemployment benefit, or other compensatory arrangement.

4. *Director* shall have the meaning described in 12 CFR 215.2(d).[3]

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

6. *Principal shareholder* shall have the meaning described in 12 CFR 215.2(m).[5]

II. Operational and Managerial Standards

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

1. An organizational structure that establishes clear lines of authority and responsibility for monitoring adherence to established policies;

2. Effective risk assessment;

3. Timely and accurate financial, operational and regulatory reports;

4. Adequate procedures to safeguard and manage assets; and

5. Compliance with applicable laws and regulations.

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

1. Adequate monitoring of the system of internal controls through an internal audit function. For an institution whose size, complexity or scope of operations does not warrant a full scale internal audit function, a system of independent reviews of key internal controls may be used;

2. Independence and objectivity;

3. Qualified persons;

4. Adequate testing and review of information systems;

5. Adequate documentation of tests and findings and any corrective actions;

6. Verification and review of management actions to address material weaknesses; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

G. *Asset quality.* An insured depository institution should establish and maintain a system that is commensurate with the institution's size and the nature and scope of its operations to identify problem assets and prevent deterioration in those assets. The institution should:

1. Conduct periodic asset quality reviews to identify problem assets;
2. Estimate the inherent losses in those assets and establish reserves that are sufficient to absorb estimated losses;
3. Compare problem asset totals to capital;
4. Take appropriate corrective action to resolve problem assets;
5. Consider the size and potential risks of material asset concentrations; and
6. Provide periodic asset reports with adequate information for management and the board of directors to assess the level of asset risk.

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

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

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

A. Excessive Compensation

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

B. Compensation Leading to Material Financial Loss

Compensation that could lead to material financial loss to an institution is prohibited as an unsafe and unsound practice.

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

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

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

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

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

Appendix B to Part 364—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, 12 U.S.C. 1831p–1, and sections 501 and 505(b), 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines also address standards with respect to the proper disposal of consumer information pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w).

A. *Scope.* The Guidelines apply to customer information maintained by or on behalf of, and to the disposal of consumer information by or on the behalf of, entities over which the Federal Deposit Insurance Corporation (FDIC) has authority. Such entities, referred to as ''insured depository institution'' or ''institution'' are banks insured by the FDIC (other than members of the Federal Reserve System), state savings associations insured by the FDIC, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

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

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

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

a. *Board of directors,* in the case of a branch or agency of a foreign bank, means the managing official in charge of the branch or agency.

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

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

(A) A consumer report that an institution obtains;

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

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

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

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

(2) *Consumer information* does not include:

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

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

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

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

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

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

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

II. Standards for Information Security

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

B. *Objectives.* An institution's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information;

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and

4. Ensure the proper disposal of customer information and consumer information.

III. Development and Implementation of Information Security Program

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

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

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

B. *Assess Risk.*

Each institution shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. *Manage and Control Risk.* Each institution shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities. Each institution must consider whether the following security measures are appropriate for the institution and, if so, adopt those measures the institution concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program;

e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the institution's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the institution's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

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

D. *Oversee Service Provider Arrangements.* Each institution shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the institution's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, an institution should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each institution shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. *Report to the Board.* Each institution shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the institution's compliance with these Guidelines. The report, which will vary depending upon the complexity of each institution's program should discuss material matters related to its program, addressing issues such as: Risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.

G. *Implement the Standards.* 1. *Effective date.* Each institution must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that an institution has entered into with a service provider to perform services for it or functions on its behalf, satisfies the provisions of paragraph III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information as long as the institution entered into the contract on or before March 5, 2001.

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

4. *Exception for existing agreements with service providers relating to the disposal of consumer information.* Notwithstanding the requirement in paragraph III.G.3., an institution's contracts with its service providers that have access to consumer information and that may dispose of consumer information, entered into before July 1, 2005, must comply with the provisions of the Guidelines relating to the proper disposal of consumer information by July 1, 2006.

Supplement A to Appendix B to Part 364 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

I. Background

This Guidance [1] interprets section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information Security Standards (the Security Guidelines) [2] and describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The scope of, and definitions of terms used in, this Guidance are identical to those of the Security Guidelines. For example, the term ''customer information'' is the same term used in the Security Guidelines, and means any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution.

A. Interagency Security Guidelines

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

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

B. Risk Assessment and Controls

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

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

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

c. The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.[3]

2. Following the assessment of these risks, the Security Guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines,[4] and adopt those that are appropriate for the institution, including:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

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

c. Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[5]

C. Service Providers

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

II. Response Program

Millions of Americans, throughout the country, have been victims of identity theft.[7] Identity thieves misuse personal information they obtain from a number of sources, including financial institutions, to perpetrate identity theft. Therefore, financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial institutions should place access controls on customer information systems and conduct background checks for employees who are authorized to access customer information.[8] However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems [9] that occur nonetheless. A response program should be a key part of an institution's information security program.[10] The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

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

A. Components of a Response Program

1. At a minimum, an institution's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below;

c. Consistent with the Agencies' Suspicious Activity Report (''SAR'') regulations,[12] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;[13] and

e. Notifying customers when warranted.

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

III. Customer Notice

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

A. Standard for Providing Notice

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

1. Sensitive Customer Information

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

2. Affected Customers

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

B. Content of Customer Notice

1. Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance.[14] The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identify theft to the institution. The notice should include the following additional items, when appropriate:

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

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

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

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

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

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

C. Delivery of Customer Notice

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

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

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

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

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

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

[6] *See* Security Guidelines, II.B, and III.D. Further, the Agencies note that, in addition to contractual obligations to a financial institution, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission (FTC), 12 CFR part 314.

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

[8] Institutions should also conduct background checks of employees to ensure that the institution does not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).

[9] Under the Guidelines, an institution's *customer information systems* consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. *See* Security Guidelines, I.C.2.d.

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

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

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

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

[14] The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

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

PART 391—FORMER OFFICE OF THRIFT SUPERVISION REGULATIONS

■ 4. The authority citation for part 391 is revised to read as follows:

Authority: 12 U.S.C. 1819 (Tenth).

Subpart A also issued under 12 U.S.C. 1462a; 1463; 1464; 1828; 1831p–1; 1881–1884; 15 U.S.C. 1681w; 15 U.S.C. 6801; 6805.

Subpart C also issued under 12 U.S.C. 1462a; 1463; 1464; 1828; 1831p-1; and 1881–1884; 15 U.S.C. 1681m; 1681w.

Subpart D also issued under 12 U.S.C. 1462; 1462a; 1463; 1464; 42 U.S.C. 4012a; 4104a; 4104b; 4106; 4128.

Subpart E also issued under 12 U.S.C. 1467a; 1468; 1817; 1831i.

Subpart B—[Removed and Reserved]

■ 5. Remove and reserve subpart B consisting of §§ 391.10 through 391.14, appendix A to subpart B of part 391, and appendix B to subpart B of part 391.

Dated at Washington, DC, this 21st day of January, 2015.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

[FR Doc. 2015–01325 Filed 1–29–15; 8:45 am]

BILLING CODE 6714–01–P

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Parts 324 and 329

RIN 3064–AE30

Regulatory Capital Rules, Liquidity Coverage Ratio: Proposed Revisions to the Definition of Qualifying Master Netting Agreement and Related Definitions

AGENCY: Federal Deposit Insurance Corporation (FDIC).

ACTION: Notice of proposed rulemaking.

SUMMARY: The FDIC invites comment on a notice of proposed rulemaking (NPR or proposed rule) that would amend the definition of ''qualifying master netting agreement'' under the regulatory capital rules, and the liquidity coverage ratio rule. The FDIC also is proposing to amend the definitions of ''collateral agreement,'' ''eligible margin loan,'' and ''repo-style transaction'' under the regulatory capital rules. The amendments are designed to ensure that the regulatory capital and liquidity treatment of certain financial contracts generally would not be affected by implementation of special resolution regimes in foreign jurisdictions if such regimes are substantially similar to Title II of the Dodd-Frank Wall Street Reform and Consumer Protection Act and the Federal Deposit Insurance Act in the United States, or by the International Swaps and Derivative Association Resolution Stay Protocol that provide for contractual submission to such regimes. In December 2014, the Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System (Board) adopted a joint interim final rule that is related to this proposed rule.

DATES: Comments must be received March 31, 2015.

ADDRESSES: You may submit comments, identified by RIN 3064–AE30, by any of the following methods:

- *Agency Web site: http://www.fdic.gov/regulations/laws/federal/.* Follow instructions for submitting comments on the Agency Web site.
- *Email: Comments@fdic.gov.* Include the RIN 3064–AE30 on the subject line of the message.
- *Mail:* Robert E. Feldman, Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street NW., Washington, DC 20429.
- *Hand Delivery:* Comments may be hand delivered to the guard station at the rear of the 550 17th Street Building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m.

Public Inspection: All comments received must include the agency name and RIN 3064–AE30 for this rulemaking. All comments received will be posted without change to *http://www.fdic.gov/regulations/laws/federal/,* including any personal information provided. Paper copies of public comments may be ordered from the FDIC Public Information Center, 3501 North Fairfax Drive, Room E–I002, Arlington, VA 22226 by telephone at (877) 275–3342 or (703) 562–2200.

FOR FURTHER INFORMATION CONTACT: Bobby R. Bean, Associate Director, *bbean@fdic.gov;* Ryan Billingsley, Chief, Capital Policy Section, *rbillingsley@fdic.gov;* Benedetto Bosco, Capital Markets Policy Analyst, *bbosco@fdic.gov;* Capital Markets Branch, Division of Risk Management Supervision, (202) 898–6888; or David Wall, Assistant General Counsel, *dwall@fdic.gov;* Michael Phillips, Counsel, *mphillips@fdic.gov;* Ann Battle, Counsel, *abattle@fdic.gov;* Rachel Ackmann, Senior Attorney, *rackmann@fdic.gov;* Grace Pyun, Senior Attorney, *gpyun@fdic.gov;* Supervision Branch, Legal Division, Federal Deposit Insurance Corporation, 550 17th Street NW., Washington, DC 20429.

SUPPLEMENTARY INFORMATION:

I. Summary

The regulatory capital rules of the Board, the OCC, and the FDIC (collectively, the agencies) permit a banking organization to measure exposure from certain types of financial contracts on a net basis and recognize the risk-mitigating effect of financial collateral for other types of exposures, provided that the contracts are subject to a ''qualifying master netting agreement'' that provides for certain rights upon a counterparty default.[1] The agencies, by rule, have defined a qualifying master netting agreement as a netting agreement that permits a banking organization to terminate, apply close-out netting, and promptly liquidate or set-off collateral upon an event of default of the counterparty (default rights), thereby reducing its counterparty exposure and market risks.[2] On the whole, measuring the amount of exposure of these contracts on a net basis, rather than a gross basis, results in a lower measure of exposure, and thus, a lower capital requirement, under the regulatory capital rules.

The current definition of ''qualifying master netting agreement'' recognizes that default rights may be stayed if the financial company is in receivership, conservatorship, or resolution under Title II of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act),[3] or under the Federal Deposit Insurance Act (FDI Act).[4] Accordingly, transactions conducted under netting agreements where default rights may be stayed under Title II of the Dodd-Frank Act or the FDI Act may qualify for the favorable capital treatment described above. However, the current definition of ''qualifying master netting agreement'' does not recognize that default rights may be stayed where a master netting agreement is subject to limited stays under foreign special resolution regimes or where counterparties agree through contract that a special resolution regime would apply. When the agencies adopted the current definition of ''qualifying master netting agreement,'' no other jurisdiction had adopted a special resolution regime relevant to the definition, and no banking organizations

[1] See 12 CFR part 3 (OCC), 12 CFR part 217 (Board); 12 CFR part 324 (FDIC). The term ''banking organization'' includes national banks, state member banks, state nonmember banks, savings associations, and top-tier bank holding companies domiciled in the United States not subject to the Board's Small Bank Holding Company Policy Statement (12 CFR part 225, appendix C), as well as top-tier savings and loan holding companies domiciled in the United States, except for certain savings and loan holding companies that are substantially engaged in insurance underwriting or commercial activities.

[2] See section 2 of the regulatory capital rules.

[3] See 12 U.S.C. 5390(c)(8) through (16).

[4] See 12 U.S.C. 1821(e)(8) through (13). The definition also recognizes that default rights may be stayed under any similar insolvency law applicable to government sponsored enterprises (GSEs). Generally under the agencies' regulatory capital rules, government-sponsored enterprise means an entity established or chartered by the U.S. government to serve public purposes specified by the U.S. Congress but whose debt obligations are not explicitly guaranteed by the full faith and credit of the U.S. government. See regulatory capital rules Section 2.