DEPARTMENT OF THE TREASURY
Office of the Comptroller of the Currency
12 CFR Parts 30 and 41
Docket No. 04-13
RIN 1557-AC84

FEDERAL RESERVE SYSTEM
12 CFR Parts 208, 211, 222, and 225
Docket No. R-1199

FEDERAL DEPOSIT INSURANCE CORPORATION
12 CFR Parts 334 and 364
RIN 3064-AC77

DEPARTMENT OF THE TREASURY
Office of Thrift Supervision
12 CFR Parts 568, 570, and 571
No. 2004-56
RIN 1550-AB87

Proper Disposal of Consumer Information under the Fair and Accurate Credit Transactions Act of 2003

AGENCIES: Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); and Office of Thrift Supervision, Treasury (OTS).

ACTION: Final rule.

SUMMARY: The OCC, Board, FDIC, and OTS (the Agencies) are adopting a final rule to implement section 216 of the Fair and Accurate Credit Transactions Act of 2003 by amending the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. The final rule generally requires each financial institution to develop, implement, and maintain, as part of its existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports to address the risks associated with identity theft.

EFFECTIVE DATE: July 1, 2005.

FOR FURTHER INFORMATION CONTACT:

OCC: Aida Plaza Carter, Director, Bank Information Technology, (202) 874-4740; Amy Friend, Assistant Chief Counsel, (202) 874-5200; or Deborah Katz, Senior Counsel, Legislative and Regulatory Activities Division, (202) 874-5090.

Board: Donna L. Parker, Supervisory Financial Analyst, Division of Supervision & Regulation, (202) 452-2614; Joshua H. Kaplan, Attorney, Legal Division, (202) 452-2249; Minh-Duc T. Le or Ky Tran-Trong, Senior Attorneys, Division of Consumer and Community Affairs, (202) 452-3667.

FDIC: Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898-3872; Kathryn M. Weatherby, Examination Specialist, Division of Supervision and Consumer Protection, (202) 898-6793; Robert A. Patrick, Counsel, Legal Division, (202) 898-3757; Janet V. Norcom, Counsel, Legal Division, (202) 898-8886.

OTS: Glenn Gimble, Senior Project Manager, Thrift Policy, (202) 906-7158; Lewis C. Angel, Senior Project Manager, Technology Risk Management, (202) 906-5645; Richard Bennett, Counsel (Banking and Finance), Regulations and Legislation Division, (202) 906-7409.

SUPPLEMENTARY INFORMATION:

I. Introduction

Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act or the Act) adds a new section 628 to the Fair Credit Reporting Act (FCRA), at 15 U.S.C. 1681w, that, in general, is designed to protect a consumer against the risks associated with unauthorized access to information about the consumer contained in a consumer report, such as fraud and related crimes including identity theft. Section 216 of the Act requires each of the Agencies to adopt a regulation with respect to the entities that are subject to its enforcement authority "requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation." Pub. L. 108-159, 117 Stat. 1985-86. The FACT Act mandates that the Agencies ensure that their respective regulations are consistent with the requirements issued pursuant to the Gramm-Leach-Bliley Act (GLB Act) (Pub. L. 106-102), as well as other provisions of federal law.

On June 8, 2004, the Agencies published a proposal to amend the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) to require financial institutions to implement controls designed to ensure the proper disposal of "consumer information" within the meaning of section 216.[1] A total of 68 comments on the proposal were submitted to the Agencies, some of which were submitted to more than one of the Agencies. Most of these comments were submitted by financial institutions and associations that represent them. A few comments were submitted by trade associations from the information destruction industry.[2]

In general, commenters expressed support for the Agencies' proposal because the new requirements would allow financial institutions sufficient latitude to adopt controls that suit their particular circumstances. Commenters offered revisions to several aspects of the proposal, notably the definitions and compliance deadlines, and the Agencies have considered each of these suggestions.

The Agencies also proposed to amend their respective regulations that implement the FCRA by adding a new provision setting forth the duties of users of consumer reports regarding identity theft. The proposed provision would require a financial institution to properly dispose of consumer information in accordance with the standards set forth in the Guidelines. The Agencies also proposed to amend their respective FCRA regulations by incorporating a rule of construction, which generally provides that the duty to properly dispose of consumer information shall not be construed to require a financial institution

---

[1] 69 FR 31913 (June 8, 2004). The Guidelines are codified at 12 CFR Parts 30, app. B (OCC); 208, app. D-2 and 225, app. F (Board); 364, app. B (FDIC); 570, app. B (OTS). Citations to the Guidelines omit references to titles and publications and give only the appropriate paragraph or section number.

[2] Individual consumers and organizations representing consumers submitted comments on the proposed rule issued by the Federal Trade Commission (FTC), which was substantively similar to the Agencies' proposal. 69 FR 21388 (April 20, 2004); see http://www.ftc.gov/os/comments/disposal/index.htm. The Agencies have reviewed these and other comments submitted to the FTC in connection with this final rule.

to maintain or destroy any record pertaining to a consumer that is not imposed under any other law or alter any requirement under any other law to maintain or destroy such a record. This rule of construction closely tracks section 628(b) of the FCRA, as added by section 216 of the FACT Act. In general, commenters supported the Agencies' proposal to amend their FCRA regulations and, in particular, urged the Agencies to retain the rule of construction in the final rule.

In accordance with section 216 of the Act, the Agencies have consulted with the FTC, the National Credit Union Administration, and the Securities and Exchange Commission to ensure that, to the extent possible, the rules adopted by the respective agencies are consistent and comparable.

II. Background

On February 1, 2001, the Agencies issued the Guidelines pursuant to sections 501 and 505 of the GLB Act (15 U.S.C. 6801 and 6805).[3] The Guidelines establish standards relating to the development and implementation of administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Guidelines apply to the financial institutions subject to the Agencies' respective jurisdictions. As mandated by section 501(b) of the GLB Act, the Guidelines require each financial institution to develop a written information security program that is 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.[4] The Guidelines direct financial institutions to assess the risks to their customer information and customer information systems and, in turn, implement appropriate security measures to control those risks.[5] For example, under the risk-assessment framework currently imposed by the Guidelines, each financial institution must evaluate whether the controls the institution has developed sufficiently protect its customer information from unauthorized access, misuse, or alteration when the institution disposes of the information.[6]

III. Proper Disposal of Consumer Information and Customer Information

To implement section 216 of the FACT Act, the Agencies are adopting amendments to the Guidelines[7] that require each financial institution to develop and maintain, as part of its information security program, appropriate controls designed to ensure that the institution properly disposes of "consumer information." The amendments to the Guidelines generally require a financial institution to properly dispose

---

[3] 66 FR 8616 (Feb. 1, 2001).

[4] Guidelines, II.B.

[5] See generally, III.B. and III.C.

[6] See 66 FR 8618. ("Under the final Guidelines, a financial institution's responsibility to safeguard customer information continues through the disposal process.")

[7] The Agencies are renaming the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" to read "Interagency Guidelines Establishing Standards for Information Security" to make clear that the Guidelines encompass the disposal of consumer information.

of "consumer information" derived from a consumer report in a manner consistent with a financial institution's existing obligations under the Guidelines to properly dispose of customer information. Although the Guidelines currently address an institution's obligations to properly dispose of customer information, the amendments now state this obligation more directly and combine it with the new requirement to properly dispose of consumer information.

The Agencies have incorporated this new requirement into the Guidelines by: (1) adding a definition of "consumer information," including illustrations of the information covered by the new term; (2) adding an objective (in paragraph II) regarding the proper disposal of customer information and consumer information; and (3) adding a provision (in paragraph III) that requires a financial institution to implement appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements in paragraph III.

The final rule requires each financial institution to implement the appropriate measures to properly dispose of "consumer information" by July 1, 2005. The Agencies believe that any changes to an institution's existing information security program likely will be minimal because many of the measures that an institution already uses to dispose of "customer information" can be adapted to properly dispose of "consumer information." Nevertheless, a few of the comments noted that the proposed period for compliance would be relatively short in light of the work required to locate and track all "consumer information" in a financial institution's existing information systems. Accordingly, the Agencies have determined that financial institutions should be afforded a six-month period to adjust their systems and controls.

A discussion of each proposed amendment to the Guidelines and the addition of cross-references to the Guidelines in the Agencies' FCRA regulations follows.

Consumer information

The proposal defined "consumer information" to mean "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 was defined to mean "a compilation of such records."

Commenters generally supported the Agencies' proposed definition of this term, but argued that the Agencies should include statements or illustrations to clarify the nature and scope of "consumer information." Several commenters found the proposed phrase "about an individual" to be ambiguous and urged the Agencies to adopt a definition expressly stating that "consumer information" only includes information that identifies a particular individual.

Similarly, some commenters supported the Agencies' explanation in the proposal that "consumer information" does not include information derived from a consumer

report that does not identify any particular consumer, such as the mean credit score derived from a group of consumer reports. These commenters suggested that the Agencies include this example (or similar examples) in the definition.

In the final rule, as in the proposed rule, the Agencies have continued to define "consumer information" to mean "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." In addition, the Agencies have continued to define "consumer information" to mean "a compilation of such records," as proposed.

The Agencies have modified the term "consumer information," however, to expressly exclude from the definition "any record that does not identify an individual." The Agencies believe that qualifying the term "consumer information" to cover only personally identifiable information appropriately focuses on the information derived from a consumer report that, if improperly disposed, could be used to commit fraud or identity theft against a consumer. The Agencies believe that limiting "consumer information" to information that identifies a consumer is consistent with the current law relating to the scope of the term "consumer report" under the FCRA and the purposes of section 216 of the FACT Act.

Under the final rule, a financial institution must implement measures to properly dispose of "consumer information" that identifies a consumer, such as the consumer's name and the credit score derived from a consumer report. However, this requirement does not apply to aggregate information, such as the mean credit score that is derived from a group of consumer reports, or blind data, such as a series of credit scores that do not identify the subjects of the consumer reports from which those scores are derived. The Agencies have included examples of records that illustrate this aspect of the Guidelines, but have not rigidly defined the nature and scope of personally identifiable information. The Agencies note that there are a variety of types of information apart from an individual's name, account number, or address that, depending on the circumstances or when used in combination, could identify the individual.

A few commenters argued that the term "consumer information" should exclude non-sensitive information about a consumer, such as names and addresses that are publicly available. These commenters urged the Agencies to limit "consumer information" to information about an individual's specific financial characteristics, such as payment history or account numbers, or personal characteristics, such as driver's license information. In their view, only sensitive, non-public information should be subject to the requirements of the rule because unauthorized access to or misuse of that information poses the greatest threats of identity theft against consumers. The Agencies believe that there is no basis to exclude certain classes of relatively non-sensitive information from the scope of "consumer information" under section 216 of the Act.

Some commenters urged the Agencies to eliminate references to business-related transactions in the discussion of the definition of "consumer information." These

commenters argued that the FCRA defines a "consumer report" only with respect to information used to determine a consumer's eligibility for "credit or insurance to be used primarily for personal, family, or household purposes."[8] Thus, these commenters recommended that the Agencies remove references to business transactions that, in their view, would be inconsistent with the scope of the FCRA. The Agencies note that the FCRA defines a "consumer report" as encompassing a communication by a consumer reporting agency of information about a consumer that, in general, is used as a factor in establishing the consumer's eligibility for "any other purpose authorized under section 604 [of the FCRA]." [9] Among other permissible purposes, a consumer reporting agency lawfully may furnish a consumer report to a person which it has reason to believe "otherwise has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer."[10] If used in whole or in part to establish a consumer's eligibility for a business transaction that is initiated by the consumer, such as an application for a small business loan that is initiated by a sole proprietor, then that information could be a consumer report. Accordingly, a financial institution that maintains information derived from a consumer report for a business purpose including a consumer report originally obtained in connection with a "business transaction that is initiated by the consumer," would be subject to the requirement to properly dispose of such information, pursuant to section 216 of the FACT Act.

As discussed in the proposal, the Agencies note that the scope of information covered by the terms "consumer information" and "customer information" will sometimes overlap, but will not always coincide. The definition of "consumer information" is drawn from the term "consumer" in section 603(c) of the FCRA, which defines a "consumer" as an individual, without elaboration. 15 U.S.C. 1681a(c). By contrast, "customer information" under the Guidelines, means nonpublic personal information about a "customer," namely, an individual who obtains a financial product or service to be used primarily for personal, family, or household purposes and who has a continuing relationship with the financial institution.[11]

The relationship between "consumer information" and "customer information" can be illustrated through the following examples. Payment history information from a consumer report about an individual, who is a financial institution's customer, will be both "consumer information" because it comes from a consumer report and "customer information" because it is nonpublic personal information about a customer. In some circumstances, "customer information" will be broader than "consumer information." For instance, information about a financial institution's own transactions with its customer is "customer information" but is not "consumer information" because it does not come from a consumer report. In other circumstances, "consumer information" will be broader than "customer information." "Consumer information" includes information from a consumer report that an institution obtains about an individual who applies for but does not receive a loan, an individual who guarantees a loan (including a loan to a

[8] 15 U.S.C. 1681a(d)(1)(A).
[9] 15 U.S.C. 1681a(d)(1)(C).
[10] 15 U.S.C. 1681b(a)(3)(F)(i).
[11] I.C.2.b.

business entity), an employee or a prospective employee, or an individual in connection with a loan to the individual's sole proprietorship. In each of these instances, the consumer reports are not "customer information" because the information is not about a "customer" within the meaning of the Guidelines.

The Agencies believe that the phrase "derived from consumer reports" covers all of the information about a consumer that is taken from a consumer report, including information that results in whole or in part from manipulation of information from a consumer report or information from a consumer report that has been combined with other types of information. Consequently, a financial institution that possesses any of this information must properly dispose of it. For example, any record about a consumer derived from a consumer report, such as the consumer's name and credit score, that is shared among affiliates must be disposed of properly by each affiliate that possesses that information.[12] Similarly, a consumer report that is shared among affiliated companies after the consumer has been given a notice and has elected not to opt out of that sharing, and therefore is no longer a "consumer report" under the FCRA,[13] would still be "consumer information." Accordingly, an affiliate that receives "consumer information" under these circumstances must properly dispose of the information.

A few commenters suggested that the Agencies modify this provision to limit the obligation of a financial institution to properly dispose of consumer information only when the institution knows that the information has been derived from a consumer report. The Agencies believe that implementing such a limitation is unwarranted in light of the general duty established in section 216 of the Act which applies to "any person that maintains or otherwise possesses consumer information," without regard to whether the person actually knows that it possesses such information.

The Agencies note that the proposed definition of "consumer information" includes the qualification "for a business purpose," as set forth in section 216 of the Act. The Agencies believe that the phrase "for a business purpose" encompasses any commercial purpose for which a financial institution might maintain or possess "consumer information." Commenters did not raise concerns about this interpretation.

Some commenters urged the Agencies to define the term "disposal" to clarify whether the sale, donation, or transfer of any medium containing "consumer information" is covered by the requirements imposed under the Guidelines. A few other commenters, however, disagreed with this suggestion and supported the Agencies' proposal, which was silent with respect to this particular term. The Agencies believe that there is no need to adopt a definition of the term "disposal" because, in the context of the duty imposed under section 216 of the FACT Act, the ordinary meaning of that term applies. The

---

[12] An affiliate subject to the jurisdiction of the OCC, Board, FDIC, or OTS must properly dispose of consumer information that it possesses or maintains in accordance with the agency's rule. An affiliate subject to the jurisdiction of the FTC or the SEC must properly dispose of consumer information that it possesses or maintains in accordance with the FTC's or SEC's final rules, as applicable, which are consistent and comparable to this final rule. Savings associations and savings association subsidiaries that are not functionally regulated are subject to the OTS's Guidelines.

[13] 15 U.S.C. 1681a(d)(2)(A)(iii).

Agencies note that any sale, lease, or other transfer of any medium containing "consumer information" constitutes disposal of the information insofar as the information itself is not the subject of the sale, lease, or other transfer between the parties. By contrast, the sale, lease, or other transfer of consumer information from a financial institution to another party (which may be subject to limitations imposed under other laws) can be distinguished from the act of throwing out or getting rid of consumer information, and accordingly, does not constitute "disposal" that is subject to the Agencies' rule.

New Objective for an Information Security Program

The Agencies proposed to add a new objective regarding the proper disposal of consumer information in paragraph II.B. of the Guidelines. A few commenters expressed objections to this aspect of the proposal, mainly insofar as this provision relates to service providers.

Under the final rule, a financial institution must design its information security program to satisfy the general objective to "[e]nsure the proper disposal of customer information and consumer information." The added reference to "customer information" more directly states an institution's overall duties with respect to disposing of information. However, because proper disposal of customer information already is part of a financial institution's obligation in designing and maintaining its information security program under the Guidelines, the inclusion of "customer information" in the objective does not impose a new requirement on an institution's compliance with the Guidelines.

The general objective to "[e]nsure the proper disposal of customer information and consumer information" replaces the proposed provision that would require an institution to develop controls "in a manner consistent with the disposal of customer information." The Agencies believe that setting forth the obligation in this manner more directly states a financial institution's obligation to develop and maintain risk-based measures to dispose of both types of information properly and is consistent with the Guidelines and the Act.

The Agencies continue to believe that imposing this additional objective in paragraph II.B is important because this disposal requirement applies to a financial institution's "consumer information" maintained or otherwise in the possession of the institution's service providers. The Guidelines require, in part, that a financial institution "[r]equire its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines."[14]

By expressly incorporating a provision in paragraph II.B., each financial institution must contractually require its service providers to develop appropriate measures for the proper disposal of consumer information and, where warranted, to monitor its service providers to confirm that they have satisfied their contractual obligations. As several commenters observed, the particular contractual arrangements

[14] III.D.2. This requirement applies to service providers located domestically and abroad.

that an institution may negotiate with a service provider may take varied forms or use general terms. As a result, some institutions may have existing contracts that cover the proper disposal of customer information and consumer information. The Agencies continue to believe that the parties should be allowed substantial latitude in negotiating the contractual terms appropriate to their arrangement in any manner that satisfies the objectives of the Guidelines. Accordingly, the Agencies have not prescribed any particular standards that relate to this contract requirement.

The Agencies have made a technical amendment to the definition of "service provider" in paragraph I.C.2. to include a reference to "consumer information" in addition to "customer information." Thus the amended definition of service provider is "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 bank." Consistent with section 216 and the amendments to the Guidelines, a financial institution's obligation with respect to a service provider that has access to consumer information is limited to ensuring that the service provider properly disposes of consumer information.

The Agencies also have amended paragraph III.G.2. to allow a financial institution a reasonable period of time, after the final regulations are issued, to amend its contracts with its service providers to incorporate the necessary requirements in connection with the proper disposal of consumer information. After reviewing the comments on this provision of the proposal, which uniformly advocated a longer period of time for modifying contracts with service providers if necessary, the Agencies have determined that financial institutions must modify any affected contracts not later than July 1, 2006.

New Provision to Implement Measures to Properly Dispose of Consumer Information

The Agencies have amended paragraph III.C. (Manage and Control Risk) of the Guidelines by adding a new provision to require a financial institution to develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information. Like the provision described in the proposal, this new provision requires an institution to implement these measures "in accordance with each of the requirements in this paragraph III." of the Guidelines.

Paragraph III. of the Guidelines presently requires a financial institution to undertake measures to design, implement, and maintain its information security program to protect customer information and customer information systems. Because "customer information systems" is defined to include any methods used to dispose of customer information, a financial institution presently must use risk-based measures to protect customer information in the course of disposing of it. Building on this provision in the Guidelines, the Agencies proposed a provision in paragraph III.C. that would require a financial institution to develop controls "in a manner consistent with the disposal of customer information." Commenters generally supported this provision because a

financial institution would be permitted to develop and implement risk-based protections, rather than adopt particular methods for disposing of consumer information that would comply with a prescriptive standard.

Under the final rule, an institution must adopt procedures and controls to properly dispose of "consumer information" and "customer information." Instead of describing a financial institution's obligation to dispose of "consumer information" in relation to the standard for "customer information" (which is currently set forth in discrete provisions of the Guidelines), the Agencies have determined that the obligation should be stated directly and generally. A provision that requires each financial institution to develop and maintain risk-based measures to properly dispose of customer information and consumer information more clearly states an institution's responsibilities to properly dispose of both classes of information and is consistent with the Guidelines and the Act.

Under this provision of the final rule, a financial institution must broaden the scope of its risk assessment to include an assessment of the reasonably foreseeable internal and external threats associated with the methods it uses to dispose of "consumer information," and adjust its risk assessment in light of the relevant changes relating to such threats. By expressly adding this new provision, the Agencies are requiring a financial institution to integrate into its information security program each of those risk-based measures in connection with the disposal of "consumer information," as set forth in paragraph III. of the Guidelines.

Some commenters urged the Agencies to adopt a detailed standard for the destruction of information or criteria that define "proper" methods or levels of disposal, rather than a provision that tracks the general obligation imposed under section 216 of the FACT Act. Other commenters favored the approach set forth in the proposal and argued that the general duty to "properly dispose of consumer information" is appropriately suited to the varying circumstances that financial institutions confront.

After reviewing the comments, the Agencies continue to believe that it is not necessary to propose a prescriptive rule describing proper methods of disposal. Nonetheless, consistent with interagency guidance previously issued through the Federal Financial Institutions Examination Council (FFIEC),[15] the Agencies expect institutions to have appropriate disposal procedures for records maintained in paper-based or electronic form. The Agencies note that an institution's information security program should ensure that paper records containing either customer or consumer information should be rendered unreadable as indicated by the institution's risk assessment, such as by shredding or any other means. Institutions also should recognize that computer-based records present unique disposal problems. Residual data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive electronic data.[16]

---

[15] See FFIEC Information Technology Examination Handbook, Information Security Booklet, page 63 at: http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf.

[16] See id.

Proposed Amendments to the Agencies' FCRA Regulations

As set forth in the proposal, the Agencies' final rules create a cross-reference to the Guidelines in their respective regulations that implement the FCRA[17] by adding a provision setting forth the duties of users of consumer reports regarding identity theft. Commenters generally agreed with the Agencies' proposal to create the cross-reference. In particular, commenters supported the Agencies' proposal to make explicit in the regulations the rule of construction in the statute stating that the requirement pertaining to proper disposal under the FCRA shall not be construed as requiring a person to maintain or destroy a record containing consumer information and does not alter any requirement imposed under other law to maintain or destroy such a record.

The new provision requires a financial institution to properly dispose of consumer information in accordance with the standards set forth in the Guidelines. This provision applies to an institution to the extent that the institution is covered by the scope of the Guidelines.[18] The provision also incorporates a rule of construction that closely tracks the terms of section 628(b) of the FCRA, as added by section 216 of the FACT Act.[19]

IV. Regulatory Analysis

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) and its implementing regulations at 5 CFR 1320, including Appendix A.1, the Agencies have reviewed the final rules and determined that they contain no collections of information. The Board made this determination under authority delegated by the Office of Management and Budget.

Regulatory Flexibility Act

In accordance with the Regulatory Flexibility Act, each agency must publish a final regulatory flexibility analysis with its final rule, unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities. (5 U.S.C. 601-612). Each of the Agencies hereby certifies that its final rule does not have a significant economic impact on a substantial number of small entities.

The rules require a financial institution subject to the jurisdiction of the appropriate agency to implement appropriate controls designed to ensure the proper

[17] 12 CFR part 41 (OCC); 12 CFR part 222 (Board); 12 CFR part 334 (FDIC); and 12 CFR part 571 (OTS). Several of the Agencies proposed establishing new parts to house their respective regulations implementing the FCRA in a notice of proposed rulemaking titled "Fair Credit Reporting Medical Information Regulations." See 69 FR 23380 (April 28, 2004). As these regulations are not yet final, the new parts are established in this final rule.

[18] Bank holding companies will be subject to the FTC's disposal rule (16 CFR Part 682) and functionally regulated subsidiaries of financial institutions will be subject to the SEC's disposal rule (17 CFR Part 248) or the FTC's disposal rule, as applicable.

[19] The OTS is making additional conforming changes to its regulations at 12 CFR 568.1 and 568.5, as well.

disposal of "consumer information." A financial institution must develop and maintain these controls as part of implementing its existing information security program for "customer information," as required under the Guidelines.[20]

Any modifications to a financial institution's information security program needed to address the proper disposal of "consumer information" could be incorporated through the process the institution presently uses to adjust its program under paragraph III.E. of the Guidelines, particularly because of the similarities between customer information and consumer information and the measures commonly used to properly dispose of both types of information. To the extent that these rules impose new requirements for certain types of "consumer information," developing appropriate measures to properly dispose of that information likely would require only a minor modification of an institution's existing information security program.

Because some "consumer information" will be "customer information" and because segregating particular records for special treatment may entail considerable costs, the Agencies believe that many banks and savings associations, including small institutions, already are likely to have implemented measures to properly dispose of both "customer" and "consumer" information. In addition, the Agencies, through the Federal Financial Institutions Examination Council (FFIEC), already have issued guidance regarding their expectations concerning the proper disposal of all of an institution's paper and electronic records. See FFIEC Information Technology Examination Handbook, Information Security Booklet, December 2002, p. 63.[21] Therefore, the rules do not require any significant changes for institutions that currently have procedures and systems designed to comply with this guidance.

The Agencies anticipate that, in light of current practices relating to the disposal of information in accordance with the Guidelines and the guidance issued by the FFIEC, the final rules will not impose undue costs on financial institutions. Therefore, the Agencies believe that the controls that small financial institutions will develop and implement, if any, to comply with the rules likely pose a minimal economic impact on those entities.

FDIC – Small Business Regulatory Enforcement Fairness Act

The Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) (Public Law 104-121, 110 Stat. 857) provides generally for agencies to report rules to Congress and for Congress to review these rules. The reporting requirement is triggered in instances where the FDIC issues a final rule as defined by the Administrative Procedure Act (APA) (5 U.S.C. 551, et seq.). Because the FDIC is issuing a final rule as defined by the APA, the FDIC will file the reports required by SBREFA.

OCC and OTS Executive Order 12866 Determination

[20] In 2001, the Agencies issued final Guidelines requiring financial institutions to develop and maintain an information security program, including procedures to dispose of customer information, and each agency provided a final regulatory flexibility analysis at that time. See 66 FR 8625-32 (Feb. 1, 2001).

[21] See footnote 15, supra.

The OCC and OTS each have determined that this rule is not a "significant regulatory action" under Executive Order 12866.

OCC and OTS Unfunded Mandates Reform Act of 1995 Determination

Under Section 202 of the Unfunded Mandates Reform Act of 1995, Public Law 104-4 (2 U.S.C. 1532) (Unfunded Mandates Act), the OCC and OTS must prepare budgetary impact statements before promulgating any rule likely to result in a federal mandate that may result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector of $100 million or more in any one year. If a budgetary impact statement is required, under section 205 of the Unfunded Mandates Act, the OCC and OTS must identify and consider a reasonable number of regulatory alternatives before promulgating a rule.

For the reasons outlined earlier, the OCC and OTS have determined that this proposal will not result in expenditures by state, local, and tribal governments, or by the private sector, of $100 million or more, in any one year. Accordingly, a budgetary impact statement is not required under section 202 of the Unfunded Mandates Reform Act of 1995 and this rulemaking requires no further analysis under the Unfunded Mandates Act.

List of Subjects

12 CFR Part 30

Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 41

Banks, banking, Consumer protection, National Banks, Reporting and recordkeeping requirements.

12 CFR Part 208

Banks, banking, Consumer protection, Information, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 211

Exports, Foreign banking, Holding companies, Reporting and recordkeeping requirements.

12 CFR Part 222

Banks, banking, Holding companies, state member banks.

12 CFR Part 225

Banks, banking, Holding companies, Reporting and recordkeeping requirements.

12 CFR Part 334

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

12 CFR Part 364

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

12 CFR Part 568

Consumer protection, Privacy, Reporting and recordkeeping requirements, Savings associations, Security measures.

12 CFR Part 570

Accounting, Administrative practice and procedure, Bank deposit insurance, **Consumer protection**, Holding companies, **Privacy**, Reporting and recordkeeping requirements, **Safety and soundness**, Savings associations.

12 CFR Part 571

Consumer protection, Credit, **Fair Credit Reporting Act**, **Privacy**, Reporting and recordkeeping requirements, Savings associations.

Department of the Treasury

Office of the Comptroller of the Currency

12 CFR CHAPTER I

Authority and Issuance

For the reasons discussed in the joint preamble, the Office of the Comptroller of the Currency amends chapter V of title 12 of the Code of Federal Regulations by amending 12 CFR part 30 and adding a new part 41 as follows:

PART 30 – SAFETY AND SOUNDNESS STANDARDS

1. The authority citation for part 30 is revised to read as follows:

Authority: 12 U.S.C. 93a, 1818, 1831-p and 3102(b); 15 U.S.C. 1681s, 1681w, 6801, and 6805(b)(1).

2. Appendix B to part 30 is amended by:

a. Revising the heading for Appendix B to part 30 entitled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" to read "Interagency Guidelines Establishing Information Security Standards" wherever it appears in Title 12, Chapter 2, part 30;
b. Revising paragraph I. Introduction;
c. Revising paragraph I.A. by adding a new sentence at the end of the paragraph;
d. Redesignating paragraphs I.C.2.b. through e. as paragraphs I.C.2.d. through g., respectively;
e. Adding new paragraphs I.C.2.b. and c., and amending redesignated paragraph g.;
f. Revising the heading for paragraph II. entitled "Standards for Safeguarding Customer Information" to read "Standards for Information Security";
g. Removing in paragraph II.B.2. the word "and" at the end of the sentence;
h. Removing in paragraph II.B.3. the period at the end of the sentence and replacing it with "; and";
i. Adding a new paragraph II.B.4.;
j. Adding a new paragraph III.C.4.; and
k. Adding new paragraphs III.G.3. and 4. to read as follows:

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

* * * * *

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 also apply to the proper disposal of consumer information by or on behalf of such entities.

* * * * *

C. Definitions. * * *

2. * * *

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 bank 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 bank obtains;

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

(E) Information from a consumer report that the bank 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).

* * * * *

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 bank.

* * * * *

II. * * *

B. * * *

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

III. * * *

C. * * *

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.

* * * * *

G. Implement the Standards. * * *

3. Effective date for measures relating to the disposal of consumer information. Each bank 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 bank'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.

3. Add part 41 to read as follows:

PART 41 -- FAIR CREDIT REPORTING

Subpart A–General Provisions

Sec.

41.1 Purpose.
41.2 [Reserved]
41.3 Definitions.

Subparts B–H [Reserved]

Subpart I – Duties of Users of Consumer Reports Regarding Identity Theft

41.80-82 [Reserved]
41.83 Disposal of consumer information

Authority: 12 U.S.C. 1 et seq., 24 (Seventh), 93a, 481, 484, and 1818; 15 U.S.C. 1681s, 1681w, 6801 and 6805.

Subpart A–General Provisions

§ 41.1 Purpose.

(a) Purpose. The purpose of this part is to establish standards for national banks regarding consumer report information. In addition, the purpose of this part is to specify the extent to which national banks may obtain, use, or share certain information. This part also contains a number of measures national banks must take to combat consumer fraud and related crimes, including identity theft.

(b) [Reserved]

§ 41.2 [Reserved]

§ 41.3 Definitions.

As used in this part, unless the context requires otherwise:

(a)–(d) [Reserved]

(e) Consumer means an individual.

(f)–(n) [Reserved]

Subparts B–H [Reserved]

Subpart I–Duties of Users of Consumer Reports Regarding Identity Theft

§ 41.80-82 [Reserved]

§ 41.83 Disposal of consumer information.

(a) Definitions as used in this section. (1) Bank means national banks, Federal branches and agencies of foreign banks, and their respective operating subsidiaries.

(b) In general. Each bank must properly dispose of any consumer information that it maintains or otherwise possesses in accordance with the Interagency Guidelines Establishing Information Security Standards, as set forth in appendix B to 12 CFR part 30, to the extent that the bank is covered by the scope of the Guidelines.

(c) Rule of construction. Nothing in this section shall be construed to:

(1) Require a bank to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or

(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

[THIS SIGNATURE PAGE RELATES TO THE FINAL RULE ON THE "PROPER DISPOSAL OF CONSUMER INFORMATION UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003."]

Dated: December 16, 2004

Julie L. Willliams (signed)

Julie L. Williams,
Acting Comptroller of the Currency.

Federal Reserve System
12 CFR Chapter II
Authority and Issuance

For the reasons set forth in the joint preamble, parts 208, 211, 222, and 225 of chapter II of title 12 of the Code of Federal regulations are amended as follows:

Part 208–MEMBERSHIP OF STATE BANKING INSTITUTIONS IN THE FEDERAL RESERVE SYSTEM (REGULATION H)

1. The authority citation for 12 CFR part 208 is revised to read as follows:

Authority: 12 U.S.C. 24, 36, 92a, 93a, 248(a), 248(c), 321-338a, 371d, 461, 481-486, 601, 611, 1814, 1816, 1820(d)(9), 1823(j), 1828(o), 1831, 1831o, 1831p-1, 1831r-1, 1831w, 1831x, 1835a, 1882, 2901-2907, 3105, 3310, 3331-3351, and 3906-3909, 15 U.S.C. 78b, 78l(b), 78l(g), 78l(i), 78o-4(c)(5), 78q, 78q-1, 78w, 1681s, 1681w, 6801 and 6805; 31 U.S.C. 5318, 42 U.S.C. 4012a, 4104a, 4104b, 4106, and 4128.

2. In § 208.3 revise paragraph (d)(1) to read as follows:

§ 208.3 Application and conditions for membership in the Federal Reserve System.

* * * * *

(d) Conditions of membership. (1) Safety and soundness. Each member bank shall at all times conduct its business and exercise its powers with due regard to safety and soundness. Each member bank shall comply with the Interagency Guidelines Establishing Standards for Safety and Soundness prescribed pursuant to section 39 of the FDI Act (12 U.S.C. 1831p-1), set forth in appendix D-1 to this part, and the Interagency Guidelines Establishing Information Security Standards prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) and section 216 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681w), set forth in appendix D-2 to this part.

* * * * *

3. Amend Appendix D-2 to part 208, as follows:

a. The heading for Appendix D-2 to Part 208 entitled “Interagency Guidelines Establishing Standards for Safeguarding Customer Information” is revised to read “Interagency Guidelines Establishing Information Security Standards” wherever it appears in Title 12, Chapter 2, Part 208;

b. In section I., Introduction, a new sentence is added at the end of the introductory paragraph.
c. In section I.A., Scope, a new sentence is added at the end of the paragraph.

d. In section I.C.2., paragraphs b. through f. are redesignated as paragraphs 2.d. through 2.h., respectively, new paragraphs 2.b. and 2.c. are added and redesignated paragraph g. is amended.
e. In paragraph II. the heading entitled "Standards for Safeguarding Customer Information" is revised to read "Standards for Information Security".
f. At the end of paragraph II.B.2. the word "and" is removed.
g. At the end of paragraph II.B.3 the period is removed and replaced with "; and".
h. In section II.B. a new paragraph 4. is added.
i. In section III.C., Manage and Control Risk, a new paragraph 4. is added.
j. In section III.G., Implement the Standards, new paragraphs 3. and 4. are added.

Appendix D-2 to Part 208—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

* * * * *

I. * * *

* * * 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. * * * These Guidelines also apply to the proper disposal of consumer information by or on behalf of such entities.

* * * * *

C.***

2. * * *

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

(E) Information from a consumer report that the bank 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).

* * * * *

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 bank.

* * * * *

II.* * *

B.* * *

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

* * * * *

III.* * *

C.* * *

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 in this paragraph III.

* * * * *

G.***

3. Effective date for measures relating to the disposal of consumer information. Each bank 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 bank'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.

Part 211–INTERNATIONAL BANKING OPERATIONS (REGULATION K)

4. The authority citation for part 211 is revised to read as follows:
5.

Authority: 12 U.S.C. 221 et seq., 1818, 1835a, 1841 et seq., 3101 et seq., and 3901 et seq.; 15 U.S.C. 1681s, 1681w, 6801 and 6805.

6. In § 211.5, revise paragraph (l) to read as follows:
7.

§ 211.5 Edge and agreement corporations.

*** * * * ***

(l) Protection of customer information and consumer information. An Edge or agreement corporation shall comply with the Interagency Guidelines Establishing Information Security Standards prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) and, with respect to the proper disposal of consumer information, section 216 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681w), set forth in appendix D-2 to part 208 of this chapter.

* * * * *

6. In § 211.24, revise paragraph (i) to read as follows:

§ 211.24 Approval of offices of foreign banks; procedures for applications; standards for approval; representative-office activities and standards for approval; preservation of existing authority.

*** * * * ***

(i) Protection of customer information and consumer information. An uninsured state-licensed branch or agency of a foreign bank shall comply with the Interagency Guidelines Establishing Information Security Standards prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) and, with respect to the proper disposal of consumer information, section 216 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681w), set forth in appendix D-2 to part 208 of this chapter.

* * * * *

PART 222–FAIR CREDIT REPORTING (REGULATION V)

7. The authority citation for part 222 is revised to read as follows:

Authority: 15 U.S.C. 1681, 1681b, 1681s, 1681s-2, and 1681w.

8. In section 222.1(b)(2)(i) remove the phrase "paragraph (b)(2)" and add in its place the word "part".

9. Add a new subpart I to read as follows:

Subparts B–H [Reserved]

Subpart I–Duties of Users of Consumer Reports Regarding Identity Theft

§ 222.80-82 [Reserved]

§ 222.83 Disposal of consumer information.

(a) Definitions as used in this section. (1) You means member banks of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and agencies of foreign banks (other than Federal branches, Federal agencies and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, 611 *et seq*.).

(b) In general. You must properly dispose of any consumer information that you maintain or otherwise possess in accordance with the Interagency Guidelines Establishing Information Security Standards, as required under sections 208.3(d) (Regulation H), 211.5(l) and 211.24(i) (Regulation K) of this chapter, to the extent that you are covered by the scope of the Guidelines.

(c) Rule of construction. Nothing in this section shall be construed to:

(1) Require you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or

(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

PART 225–BANK HOLDING COMPANIES AND CHANGE IN BANK CONTROL (Regulation Y)

10. In section 225.4, revise paragraph (h) to read as follows:

§ 225.4 Corporate practices.

* * * * *

(h) Protection of customer information and consumer information. A bank holding company shall comply with the Interagency Guidelines Establishing Information Security Standards, as set forth in appendix F of this part, prescribed pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805). A bank holding company shall properly dispose of consumer information in accordance with the rules set forth at 16 CFR Part 682.

* * * * *

11. Amend Appendix F to part 225, as follows:

a. The heading for Appendix F to Part 225 entitled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" is revised to read "Interagency Guidelines Establishing Information Security Standards" wherever it appears in Title 12, Chapter 2, Part 225.

[THIS SIGNATURE PAGE RELATES TO THE FINAL RULE ON THE "PROPER DISPOSAL OF CONSUMER INFORMATION UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003."]

By order of the Board of Governors of the Federal Reserve System, December 16, 2004.

Jennifer J. Johnson (signed)
Jennifer J. Johnson
Secretary of the Board

Federal Deposit Insurance Corporation

12 CFR CHAPTER III

Authority and Issuance

For the reasons set forth in the joint preamble, the Federal Deposit Insurance Corporation amends parts 334 and 364 of chapter III of title 12 of the Code of Federal Regulations to read as follows:

PART 334–FAIR CREDIT REPORTING

Subparts A – H [Reserved]

1. The authority citation for part 334 will read as follows:

Authority: 12 U.S.C. 1818 and 1819 (Tenth); 15 U.S.C. 1681b, 1681s, and 1681w.

* * * * *

2. Add a new subpart I to read as follows:

Subpart I–Duties of Users of Consumer Reports Regarding Identity Theft

Sec.

334.80-334.82 [Reserved]
334.83 Disposal of consumer information

*** * * * ***

Subpart I– Duties of Users of Consumer Reports Regarding Identity Theft

§ 334.80-334.82 [Reserved]

§ 334.83 Disposal of consumer information. (a) In general. You must properly dispose of any consumer information that you maintain or otherwise possess in accordance with the Interagency Guidelines Establishing Information Security Standards, as set forth in appendix B to part 364 of this chapter, prescribed pursuant to section 216 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681w) and section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)), to the extent the Guidelines are applicable to you.

(b) Rule of construction. Nothing in this section shall be construed to:

(1) Require you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or
(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

* * * * *

PART 364- STANDARDS FOR SAFETY AND SOUNDNESS

3. The authority citation for part 364 is revised to read as follows:

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

4. Revise § 364.101(b) to read as follows:

§ 364.101 Standards for safety and soundness.

* * * * *

(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, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

5. In Appendix B to part 364, the following amendments are made:

a. The heading for Appendix B to part 364 entitled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" is revised to read "Interagency Guidelines Establishing Information Security Standards" wherever it appears in Title 12, Chapter 2, part 364.
b. In the Introduction, the first sentence is revised and a new sentence is added at the end of the introductory paragraph.
c. In section I.A., Scope, the first sentence is revised.
d. In section I.C.2., Definitions, paragraphs 2.b. through 2.e. are redesignated as paragraphs 2.d. through 2.g., respectively, new paragraphs 2.b. and 2.c. are added and redesignated paragraph g. is amended.
e. In paragraph II. the heading entitled "Standards for Safeguarding Customer Information" is revised to read "Standards for Information Security".
f. At the end of paragraph II.B.2. the word "and" is removed.
g. At the end of paragraph II.B.3 the period is removed and replaced with "; and".
h. In section II.B. a new paragraph 4. is added.

i. In section III.C., Manage and Control Risk, a new paragraph 4. is added.
j. In section III.G, Implement the Standards, new paragraphs 3. and 4. are added.

Appendix B to Part 364-INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

* * * * *

I. Introduction

The Interagency Guidelines Establishing Information Security Standards (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1, and sections 501 and 505(b), 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act.* * * These Guidelines 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 behalf of, entities over which the Federal Deposit Insurance Corporation (FDIC) has authority. * * *

* * * * *

I. * * *

C.* * *

2. * * *

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

(E) information from a consumer report that the bank 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).

* * * * *

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 bank.

* * * * *

II.* * *

B. Objectives. * * *

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

III.* * *

C. * * *

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.

III**. * * ***

G. * * *

3. Effective date for measures relating to the disposal of consumer information. Each bank 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

bank'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.

[THIS SIGNATURE PAGE RELATES TO THE FINAL RULE ON THE "PROPER DISPOSAL OF CONSUMER INFORMATION UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003."]

By order of the Board of Directors.

Dated at Washington, D.C., this 7th day of December, 2004.

Federal Deposit Insurance Corporation

Robert E. Feldman (signed)

Robert E. Feldman
Executive Secretary

Office of Thrift Supervision
12 CFR Chapter V
Authority and Issuance

For the reasons set forth in the joint preamble, the Office of Thrift Supervision amends chapter V of title 12 of the Code of Federal Regulations by amending parts 568 and 570 and adding a new part 571 as follows:

PART 568--SECURITY PROCEDURES

1. The authority citation for part 568 is revised to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p-1, 1881-1884; 15 U.S.C. 1681s and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

2. Revise the part heading for part 568 to read as shown above.

3. Revise the first sentence of § 568.1(a) to read as follows:

§ 568.1 Authority, purpose, and scope.

(a) This part is issued by the Office of Thrift Supervision (OTS) under section 3 of the Bank Protection Act of 1968 (12 U.S.C 1882), sections 501 and 505(b)(1) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805(b)(1)), and sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w). * * *

* * * * *

4. Revise § 568.5 to read as follows:

§ 568.5 Protection of customer information.

Savings associations and their subsidiaries (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) must comply with the Interagency Guidelines Establishing Information Security Standards set forth in appendix B to part 570 of this chapter.

PART 570—SAFETY AND SOUNDNESS GUIDELINES AND COMPLIANCE PROCEDURES

5. In the Index for part 570, the heading for Appendix B is revised by removing "Interagency Guidelines Establishing Standards for Safeguarding Customer Information", as revised by OTS's Technical Amendments Final Rule published in December 2004, and inserting "Interagency Guidelines Establishing Information Security Standards" in its place.

6. The authority citation for part 570 is revised to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p-1, 1881-1884; 15 U.S.C. 1681s and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

7. Amend § 570.1(b) by removing the phrase "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" and adding the phrase "Interagency Guidelines Establishing Information Security Standards" in its place.

8. Amend § 570.1(c) by removing the phrase "Interagency Guidelines Establishing Standards for Safeguarding Customer Information", as revised by OTS's Technical Amendments Final Rule published in December 2004, and adding the phrase "Interagency Guidelines Establishing Information Security Standards" in its place.

9. Amend § 570.2(a) by removing the phrase "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" and adding the phrase "Interagency Guidelines Establishing Information Security Standards" in its place.

10. Amend Appendix B to part 570 by:

a. Revising the heading;
b. Revising the introductory paragraph of section I. Introduction;
c. Adding a new sentence to the end of paragraph I.A. Scope;
d. Redesignating paragraphs 2.a. through 2.d. of paragraph I.C.2. Definitions as paragraphs 2.c. through 2.f., respectively, adding new paragraphs 2.a. and 2.b., and amending redesignated paragraph f.;
e. Revising the heading for section II.;
f. Removing the word "and" at the end of paragraph II.B.2.;

g. Removing the period at the end of paragraph II.B.3 and replacing it with "; and";

h. Adding a new paragraph II.B.4.;

i. Adding a new paragraph 4. to paragraph III.C. Manage and Control Risk; and

j. Adding new paragraphs 3. and 4. to paragraph III.G. Implement the Standards.

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

* * * * *

I. Introduction

The Interagency Guidelines Establishing Information Security Standards (Guidelines) set forth standards pursuant to section 39(a) of the Federal Deposit Insurance Act (12 U.S.C. 1831p-1), and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805(b)). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines also address standards with respect to the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w).

A. Scope. * * * These Guidelines also apply to the proper disposal of consumer information by or on behalf of such entities.

* * * * *

C. Definitions. * * *

2. * * *

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

i. Examples. (1) Consumer information includes:

(A) A consumer report that a savings association obtains;

(B) Information from a consumer report that you obtain from your affiliate after the consumer has been given a notice and has elected not to opt out of that sharing;

(C) Information from a consumer report that you obtain 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 you obtain about an individual who guarantees a loan (including a loan to a business entity); or

(E) Information from a consumer report that you obtain 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.

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

* * * * *

f. 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 you.

II. Standards for Information Security * * *

B. Objectives. * * *

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

III. * * *

C. Manage and Control Risk. * * *

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

* * * * *

G. Implement the Standards. * * *

3. Effective date for measures relating to the disposal of consumer information. You 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., your contracts with 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.

11. Add a new part 571 to read as follows:

PART 571–FAIR CREDIT REPORTING

Subpart A–General Provisions

Sec.

Subparts B–H [Reserved]

Subpart I–Duties of Users of Consumer Reports Regarding Identity Theft

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p-1, 1881-1884; 15 U.S.C. 1681s and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

Subpart A–General Provisions

§ 571.1 Purpose and scope.

(a) Purpose. The purpose of this part is to establish standards regarding consumer report information. In addition, the purpose of this part is to specify the extent to which you may obtain, use, or share certain information. This part also contains a number of measures you must take to combat consumer fraud and related crimes, including identity theft.

(b) Scope.

(1) [Reserved]

(2) Institutions covered. (i) Except as otherwise provided in this paragraph (b)(2), this part applies to savings associations whose deposits are insured by the Federal Deposit Insurance Corporation (and federal savings association operating subsidiaries in accordance with § 559.3(h)(1) of this chapter).

(ii) [Reserved]

(iii) [Reserved]

§ 571.2 [Reserved]

§ 571.3 Definitions.

As used in this part, unless the context requires otherwise:

(a)–(d) [Reserved]

(e) Consumer means an individual.

(f)–(n) [Reserved]

(o) You means savings associations whose deposits are insured by the Federal Deposit Insurance Corporation and federal savings association operating subsidiaries.

Subparts B–H [Reserved]

Subpart I–Duties of Users of Consumer Reports Regarding Identity Theft

§ 571.80-82 [Reserved]

§ 571.83 Disposal of consumer information.

(a) In general. You must properly dispose of any consumer information that you maintain or otherwise possess in accordance with the Interagency Guidelines Establishing Information Security Standards, as set forth in appendix B to part 570, to the extent that you are covered by the scope of the Guidelines.

(b) Rule of construction. Nothing in this section shall be construed to:

(1) Require you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or

(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

[THIS SIGNATURE PAGE RELATES TO THE FINAL RULE ON THE "PROPER DISPOSAL OF CONSUMER INFORMATION UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003."]

Dated: November 30, 2004

By the Office of Thrift Supervision,

James E. Gilleran (signed)

James E. Gilleran,

Director