FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084 AA87

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission (''FTC'' or ''Commission'') is issuing a final Safeguards Rule, as required by section 501(b) of the Gramm-Leach-Bliley Act (''G–L–B Act'' or ''Act''), to establish standards relating to administrative, technical and physical information safeguards for financial institutions subject to the Commission's jurisdiction. As required by section 501(b), the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

EFFECTIVE DATE: This rule is effective on May 23, 2003.

FOR FURTHER INFORMATION CONTACT: Laura D. Berger, Attorney, Division of Financial Practices, (202) 326–3224.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

Section A. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Pub. L. 106–102) into law. The purpose of the Act was to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. The Act permits banks to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities. Subtitle A of Title V of the Act, captioned ''Disclosure of Nonpublic Personal Information,'' limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose certain privacy policies and practices with respect to its information sharing with both affiliates and nonaffiliated third parties. On May 12, 2000, the Commission issued a final rule, Privacy of Consumer Financial Information, 16 CFR part 313, which implemented Subtitle A as it relates to these requirements (hereinafter ''Privacy Rule'').[1] The Privacy Rule took effect on November 13, 2000, and full compliance was required on or before July 1, 2001.

Subtitle A of Title V also requires the Commission and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.[2] *See* 15 U.S.C. 6801(b), 6805(b)(2). As described in the Act, the objectives of these standards are to: (1) Ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. *See* 15 U.S.C. 6801(b)(1)–(3). The Act does not require all of the agencies to coordinate in developing their safeguards standards, and does not impose a deadline to establish them.[3] Although the Act permits most of the agencies to develop their safeguards standards by issuing guidelines, it requires the SEC and the Commission to proceed by rule.[4]

On September 7, 2000, the Commission issued for publication in the **Federal Register** a Advanced Notice of Proposed Rulemaking (''the ANPR'') on the scope and potential requirements of a Safeguards Rule for the financial institutions subject to its jurisdiction.[5] The Commission received thirty comments in response to the ANPR. Based on these comments, as well as the safeguards standards already issued by the other GLB agencies, the Commission issued a Notice of Proposed Rulemaking respecting Standards for Safeguarding Customer Information (''the proposal'' or ''the Proposed Rule'') on August 7, 2001.[6] In response to the proposal, the Commission received forty-four comments from a variety of interested parties. The Commission now issues a final rule governing the safeguarding of customer records and information for the financial institutions subject to its jurisdiction (''Safeguards Rule'').

Like the proposal, the Final Rule requires each financial institution to develop a written information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. As described below, each information security program must include certain basic elements to ensure that it addresses the relevant aspects of a financial institution's operations and that it keeps pace with developments that may have a material impact on its safeguards. In developing the Final Rule, the Commission carefully weighed the comments, including concerns expressed about the ability of smaller and less sophisticated financial institutions to meet the Rule's requirements. It also sought to ensure that the Rule mirrored the requirements of the guidelines already established by the NCUA and the other banking agencies (collectively, ''the Banking Agency Guidelines''),[7] with adjustments as needed to clarify the Rule's scope and accommodate the diverse range of entities covered by the Commission's Rule. The Commission believes that the Final Rule strikes an appropriate balance between allowing flexibility to financial institutions and establishing standards for safeguarding customer information that are consistent with the Act's goals. As described below, the Commission will issue educational materials in connection with the Rule in order to assist businesses—and in particular, small entities—to comply with its requirements without imposing undue burdens.

[1] The rule was published in the **Federal Register** at 65 FR 33646 (May 24, 2000).

[2] The other agencies responsible for establishing safeguards standards are: the Office of the Comptroller of the Currency (''OCC''); the Board of Governors of the Federal Reserve System (''Board''); the Federal Deposit Insurance Corporation (''FDIC''); the Office of Thrift Supervision (''OTS''); the National Credit Union Administration (''NCUA''); the Secretary of the Treasury (''Treasury''); and the Securities and Exchange Commission (''SEC'').

[3] By contrast, section 504 of the Act required the Agencies to work together to issue consistent and comparable rules to implement the Act's privacy provisions.

[4] The NCUA and the remaining banking agencies—the OCC, the Board, the FDIC, and OTS—have already issued final guidelines that are substantively identical. 66 FR 8152 (Jan. 30, 2001); 66 FR 8616 (Feb. 1, 2001). The SEC also adopted a final safeguards rule as part of its Privacy of Consumer Financial Information Final Rule (hereinafter ''SEC rule''). *See www.sec.gov/rules/final/34–42974.htm* (June 29, 2000).

[5] 65 FR 54186.

[6] 66 FR 41162. In addition to considering the Banking Agency Guidelines, the Commission also considered the Final Report that was issued by the Federal Trade Commission Advisory Committee on Online Access and Security on May 15, 2000 (''Advisory Committee's Report'' or ''ACR''). Although the Advisory Committee's Report addressed security only in the online context, the Commission believes that its principles have general relevance to information safeguards.

[7] *See supra* n.4.

Section B. Overview of Comments Received

The comments received were submitted by a variety of interested parties: [8] twenty-eight were from trade or other associations or companies related to financial or Internet-related services; [9] six were from corporations or associations related to higher education or the funding of student loans; [10] five were from individuals; [11] three were from information security companies; [12] two were from consumer reporting agencies; [13] and one was from a non-profit association of consumer agencies.[14]

The majority of commenters supported the proposal overall, citing its flexibility [15] and similarity to the Banking Agency Guidelines.[16] However, as discussed below, commenters expressed different views on issues concerning the Rule's scope—in particular, whether financial institutions should be responsible for the safeguards of their affiliates and service providers and whether the Rule should apply to a financial institution that has no customer relationship but receives customer information from another financial institution. In addition, a number of commenters asked that compliance with alternative standards be deemed compliance with the Rule and/or sought to exclude certain entities from the Rule's definition of ''service provider.'' Finally, numerous commenters urged that the Commission provide guidance to businesses—particularly smaller businesses—on how to comply with the Rule without incurring undue expense.[17] As discussed in detail below, comments on all of these issues were instrumental in shaping the Final Rule.

Additional comments, and the Commission's responses thereto, are discussed in the following Section-by-Section analysis.

Section C. Section-by-Section Analysis

Consistent with the proposal, the Safeguards Rule will be part 314 of 16 CFR, to be entitled ''Standards for Safeguarding Customer Information.'' This Part will follow the Privacy Rule, which is contained in part 313 of 16 CFR. The following is a section-by-section analysis of the Final Rule.

Section 314.1: Purpose and Scope

Paragraph 314.1(a) states that the Rule is intended to establish standards for financial institutions to develop, implement and maintain administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. This paragraph also states the statutory authority for the proposed Rule. No comments addressed this provision, and the Commission has made no changes to it.

Paragraph 314.1(b) sets forth the scope of the Rule, which applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction. Because, as noted below, ''financial institution'' is defined as it is in section 509(3)(A) of the Act and the Privacy Rule, the Rule covers a wide range of entities, including: non-depository lenders; consumer reporting agencies; debt collectors; data processors; courier services; retailers that extend credit by issuing credit cards to consumers; personal property or real estate appraisers; check-cashing businesses; mortgage brokers, and any other entity that meets this definition.[18] Consistent with the proposal, the Safeguards Rule covers any financial institution that is handling ''customer information''—*i.e.,* not only financial institutions that collect nonpublic personal information from their own customers, but also financial institutions that receive customer information from other financial institutions.

Comments were split on whether the Rule should apply to customer information that a financial institution receives from another financial institution. A number of commenters agreed that such recipients should be required to maintain safeguards, citing the added protections provided by this requirement.[19] However, one of these commenters expressed concern that a recipient financial institution could be subject to multiple safeguards standards or even required to prepare multiple written safeguards plans if that financial institution also acts as a service provider or is subject to other laws, such as the Fair Credit Reporting Act, that impose confidentiality requirements.[20] In addition, some commenters opposed covering recipients on the grounds that such coverage is: (1) Beyond the intent of section 501(a), which refers to a financial institution's obligation to ''its customers;'' (2) unnecessary in light of the Rule's separate treatment of service providers and affiliates; and/or (3) too burdensome.[21]

After considering the comments, the Commission has determined that covering recipient financial institutions is consistent with the purpose and language of the Act. The Commission believes that imposing safeguards obligations as to customer information that a financial institution receives about another institution's customers is the most reasonable reading of the statutory language and clearly furthers the express congressional policy to

[8] These comments are available on the Commission's Web site, at www.ftc.gov.

[9] ACA International (''ACA''); America's Community Bankers (''ACB''); Associated Credit Bureaus, now renamed the Consumer Data Industry Association (''CDIA''); BITS/Financial Services Roundtable (''BITS''); Commerce Bankshares, Inc.; Credit Union Nat'l Ass'n (''CUNA''); Council of Ins. Agents and Brokers; Debt Buyers Ass'n (''DBA''); Ernst & Young LLP (''Ernst & Young''); Financial Planning Ass'n (''FPA''); Household Finance Corporation (''Household''); Independent Community Bankers of America (''ICB''); Independent Ins. Agents of America (''Indep. Ins. Agents''); Intuit Inc. (''Intuit''); Information Technology Ass'n of America (''ITAA''); MasterCard International (''MasterCard''); Nat'l Ass'n of Indep. Insurers (''NAII''); Nat'l Ass'n of Mutual Ins. Cos. (''NAMIC''); Nat'l Automotive Dealers Ass'n (''NADA''); Nat'l Retail Federation (''NRF''); Navy Federal Credit Union (''NFCU''); Nat'l Indep. Automobile Dealers Ass'n (''NIADA''); Navy Federal Financial Group (''NFFG''); North American Securities Administrators Ass'n, Inc. (''NASAA''); Ohio Credit Union League (''OCUL''); Oracle Corporation (''Oracle''); Software & Information Industry Ass'n (''SIIA''); Visa USA, Inc. (''Visa'').

[10] American Council on Education (''ACE''); Education Finance Council and the National Council of Higher Education Loan Programs; Nat'l Council of Higher Educ. Loan Programs, Inc.; USA Education, Inc. & Student Loan Marketing Ass'n (collectively ''Sallie Mae''); Texas Guaranteed Student Loan Corp. (''TGSL''); United Student Aid Funds, Inc. (''USA Funds'').

[11] Forest Landreth (''Landreth''); Lou Larson (''Larson''); Sheila Musgrove (''Musgrove''); David Paas (''Paas''); Norman Post (''Post'').

[12] Portogo, Inc. (''Portogo''); Tiger Testing; VeriSign, Inc. (''VeriSign'').

[13] Equifax, Inc (''Equifax''); Experian Information Solutions, Inc. (''Experian'').

[14] Nat'l Ass'n of Consumer Agency Administrators (''NACAA'').

[15] *See, e.g.,* Household at 1; Intuit at 2; ITAA at 1; NRF at 2; Sallie Mae at 2; SIIA at 3; TGSL at 1; Verisign at 2.

[16] See, e.g., Visa at 1.

[17] *See, e.g.,* ICB at 2; Musgrove at 2; NADA at 2; NIADA at 9; Paas at 4–6.

[18] Under section 313.3(k)(1) of the Privacy Rule, ''financial institution'' means: any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.

Additional examples of financial institutions are provided in section 313.3(k)(2) of the Privacy Rule.

[19] *See, e.g.,* Equifax at 1–2; Intuit at 2; NIADA at 2; TGSL at 1.

[20] Equifax at 2.

[21] *See, e.g.,* ACA at 2–3; CDIA at 3; Experian at 2; Mastercard at 2–3; NAMIC at 2–3; NRF at 3. In addition, one comment stated that numerous financial institutions that do not have customer relationships of their own could be swept into the Rule in this fashion (Visa at 4). Although no commenters identified the types of financial institutions that are likely to be so affected, the Commission envisions that such entities could include consumer reporting agencies, debt collectors, independent check cashers, automated teller machine operators, and other businesses that obtain customer information from other financial institutions to process customer data, facilitate customer transactions, or carry out transactions in a consumer context.

respect the privacy of these customers and to protect the security and confidentiality of their nonpublic personal information. Covering recipients will ensure that all financial institutions over which the Commission has jurisdiction safeguard customer information and that such safeguards are not lost merely because information is shared with a third-party financial institution.[22] The Commission also believes that the Rule's provisions for affiliates and service providers, discussed below, are not sufficient to address circumstances where information is transferred to another financial institution in the absence of a service or affiliate relationship, such as for use in debt collection or consumer reporting. Without imposing safeguards in such cases, customer information would be insufficiently protected and Congressional intent to safeguard such information would be undermined. Finally, the flexible requirements of the Rule—which allow the safeguards to vary according to the size and complexity of a financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue—permit entities to develop safeguards appropriate to their operations and should minimize any burdens on recipient entities.

Nevertheless, the Commission recognizes that financial institutions covered by its Rule also may simultaneously be subject to the Rule's requirements for service providers or affiliates.[23] For example, check printers, data processors, and real property appraisers that receive customer information as service providers for a financial institution will also be directly subject to the rule because they are themselves financial institutions.[24] However, the obligations the Rule creates for financial institutions are entirely consistent with the standard it requires them to impose on their affiliate or service provider, so that each entity ultimately is required to maintain safeguards that are appropriate in light of the relevant circumstances. Thus, a financial institution that develops an information safeguards program according to the Rule will not be faced with additional or conflicting requirements merely because it also received customer information as an affiliate or service provider.

As under the proposal, the Safeguards Rule does not cover recipients of customer information that are not financial institutions, and are also neither affiliates nor service providers as defined by the Rule. However, the Commission encourages each financial institution to take reasonable steps to assure itself that any third party to which it discloses customer information has safeguards that are adequate to fulfill any representations made by the financial institution regarding the security of customer information or the manner in which it is handled by third parties.[25]

In addition, as under the proposal, the Safeguards Rule only applies to information about a consumer who is a ''customer'' of a financial institution within the meaning of the Rule.[26] This approach is consistent with the Banking Agency Guidelines and the majority of comments that addressed this issue.[27] Although the Commission believes that limiting the Rule to information about customers is warranted by the plain language of section 501 of the Act, the Commission notes, as it did in the proposal, that protecting information about consumers may be a part of providing reasonable safeguards to ''customer information'' where the two types of information cannot be segregated reliably. Further, consistent with its mandate under section 5 of the FTC Act, the Commission expects that, as with customers, any information that a financial institution provides to a consumer will be accurate concerning the extent to which safeguards apply to them. Finally, the Commission expects that each financial institution will have in place at least the administrative or other safeguards necessary to honor any ''opt-out'' requests made by consumers under the Privacy Rule.

Other comments on the Rule's scope urged that compliance with various alternative standards should constitute compliance with the Safeguards Rule. Several such commenters urged that the Rule permit compliance with another agency's safeguards standard in lieu of the FTC's. Specifically, commenters urged that: (1) Compliance with the SEC's rule constitute compliance with the FTC Rule, so that state investment advisors covered by the FTC Rule would be subject to the same standards as federal investment advisors, which are subject to the SEC's jurisdiction;[28] (2) non-federally-insured credit unions be permitted to comply with the NCUA's guidelines instead of the FTC's Rule, so that they would be subject to the same standards as federally-insured credit unions, which are under the NCUA's jurisdiction;[29] and (3) compliance with the Banking Agency Guidelines[30] be deemed compliance for service providers that may be engaged by banks as well as by entities under the FTC's jurisdiction. In addition, other commenters requested that compliance with other laws be deemed compliance with the Rule, such as the Fair Credit Reporting Act (''FCRA'');[31] the Health Insurance Portability and Accountability Act (''HIPAA'');[32] and the Fair Debt Collection Practices Act (''FDCPA'').[33]

As discussed above in connection with recipient financial institutions and others, the Commission does not intend to impose undue burdens on entities that already are subject to comparable safeguards requirements. In particular, the Commission envisions that any entity that can demonstrate compliance with the Banking Agency Guidelines (including the substantively identical NCUA Guidelines) will also satisfy the Rule. With respect to other rules and laws that may contain some safeguards, the Commission notes that the adoption of safeguards in furtherance of such rules or laws will be weighted heavily in assessing compliance with the Rule. However, because such other rules and laws do not necessarily provide comparable protections in terms of the safeguards mandated, data covered, and range of circumstances to which protections apply, compliance with such standards will not automatically ensure compliance with the Rule. For example, an entity's compliance with the FCRA, which limits the purposes for which certain financial information may be disclosed, will not guarantee that an

[22] Under the Act, the Commission has jurisdiction over ''any other financial institution or other person that is not subject to the jurisdiction of any agency or authority.'' 15 U.S.C. Section 6805(7). Thus, the Commission does not have jurisdiction over any financial institution that is subject to another Agency's authority by the Act, including national banks, bank holding companies and savings associations the deposits of which are insured by the FDIC. *See id.* at Section 6805(a)(1)–(6).

[23] As discussed below, the FTC Rule requires financial institutions to ensure the safeguards of their affiliates and take steps to oversee their service providers' safeguards. *See* sections 314.2(b) and 314.4(d), below. What safeguards would be appropriate for an affiliate or service provider depends on the facts and circumstances, just as it would for a financial institution that is directly covered by the Rule.

[24] It should be noted that this potential overlap exists for all financial institutions that are affiliates or service providers of other financial institutions, not just recipient entities.

[25] Misrepresentations regarding these issues could violate the Privacy Rule and Section 5 of the FTC Act.

[26] The Rule incorporates the definition of ''customer'' set forth in section 313(h) of the Privacy Rule. *See* section 314.2(a).

[27] *See, e.g.,* ACA at 4; DBA at 1; Mastercard at 1–2; *but see* Intuit at 3–4; NACAA at 1.

[28] NASAA at 2.

[29] CUNA at 1; OCUL at 3.

[30] Indep. Ins. Agents at 2.

[31] CDIA at 2–3; NIADA at 3.

[32] NIADA at 3.

[33] ACA at 4–5.

entity has adopted a comprehensive information security plan as described in the Rule.

Section 314.2: Definitions

This section defines terms used in the Safeguards Rule. As under the proposal, paragraph (a) makes clear that, unless otherwise stated, terms used in the Safeguards Rule bear the same meaning as in the Commission's Privacy Rule. The remaining paragraphs (b)-(d) of this section define the terms ''customer information,'' ''information security program,'' and ''service provider,'' respectively.

In addressing this section generally, several commenters expressed concern that the definitions would be confusing to the extent that they differ from those set forth in the Privacy Rule or the Banking Agency Guidelines.[34] In response, the Commission notes that, the terms used in the Rule are consistent with those used in the Privacy Rule, and differ from those used in the Guidelines only as needed to clarify the Rule's scope and make its terms more understandable and appropriate to the diverse range of non-bank financial institutions subject to the Commission's jurisdiction. Thus, as described below, the Rule defines ''customer information'' to include information handled by affiliates. Similarly, the Rule omits definitions found in the Guidelines, such as ''Board of Directors'' or ''subsidiary,'' that are not universally applicable to entities that will be subject to the Rule.

Proposed paragraph (b) defined ''customer information'' as any record containing nonpublic personal information, as defined in paragraph 313.3(n) of the Privacy Rule, about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of a financial institution or its affiliates.'' Thus, to the extent that a financial institution shares customer information with its affiliates, the proposal required it to ensure that the affiliates maintain appropriate safeguards for the customer information at issue.

Commenters expressed varying views on whether a financial institution should be responsible for its affiliates' safeguards. Some commenters agreed that customer information held by affiliates should be protected by the Rule.[35] However, some commenters requested that affiliates that are financial institutions subject to the jurisdiction of another agency be permitted to comply with the safeguards standards of that agency in lieu of the Commission's Rule.[36] Finally, several commenters stated that the Rule should not cover affiliates at all because (1) the Act was not meant to cover any entity that is not a financial institution and some affiliates may not be financial institutions [37] or (2) the fact that the Act permits financial institutions to disclose nonpublic personal information to affiliates without providing any notice or opt out indicates that no affiliates were intended to be covered by the Act's safeguards provisions.[38]

The Commission agrees that section 501 of the Act focuses on the obligations of financial institutions. It also notes, however, that the purpose of the Act is to protect customer information, and that such information easily may be shared with companies that are affiliated and under common control with such financial institutions. Therefore, the Rule imposes obligations only on financial institutions, but gives them duties with respect to customer information shared with their affiliates. The Commission does not believe that the unrestricted sharing that the Act permits among affiliates—including affiliates that are not financial institutions—shows an intent to exclude affiliates from safeguards obligations. To the contrary, the free sharing the Act permits among affiliates warrants a coordinated and consistent approach to security. The Commission notes, however, that the duty to ensure appropriate safeguards by affiliates arises only if a financial institution shares customer information with its affiliates; therefore this obligation can, and need only be, addressed as part of such sharing arrangements. In addition, the flexible standards of the Rule permit entities to develop safeguards appropriate to their operations and the sensitivity of the information at issue and should therefore minimize burdens on affiliates. Finally, as noted above, the Commission agrees that compliance with the Banking Agency Guidelines should satisfy the safeguards standards under the Commission's Rule. Therefore, any financial institution that can demonstrate its compliance with the Guidelines will not be subject to additional requirements merely because it is an affiliate of a financial institution that is covered by the Rule.

Proposed paragraph (c) defined ''information security program'' as ''the administrative, technical, or physical safeguards'' that a financial institution uses ''to access, collect, process, store, use, transmit, dispose of, or otherwise handle customer information.'' This definition is virtually identical to the Banking Agency Guidelines' definition of ''customer information systems.'' *See* Banking Agency Guidelines, section I.C.2.d. Few comments were received on this definition. In response to one commenter who urged that this term should better describe all of the ways that ''customer information'' can be provided to others, the Commission has added the words ''distribute'' and ''protect'' to this definition.[39] At the same time, the Commission notes that the words ''otherwise handle'' are intended to cover other ways that customer information is dealt with that are not specifically mentioned in the definition. Thus, the definition is adopted with only the minor changes noted above.

Proposed paragraph (d) defined the term ''service provider'' to mean ''any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to the rule.'' This definition is virtually identical to the definition set forth in the Banking Agency Guidelines. *See* Banking Agency Guidelines, section I.C.2.e. Several commenters urged that this definition be amended to exclude particular entities from the definition of service providers, namely: (1) Accountants and auditors [40] (2) financial institutions that also provide services to banks, and are subject to examination under the Bank Service Company Act (BSCA); [41] (3) any service provider that is also an affiliate of a financial institution; [42] and (4) any service provider that receives information under the Privacy Rule's general exceptions in Sections 313.14 and 313.15, and is therefore permitted access to nonpublic personal information without need for a specific agreement concerning its reuse and redisclosure.[43]

The Commission notes that the Banking Agency Guidelines do not contain exceptions to the definition of service provider. Thus, some of the recommended exceptions could result

[34] *See, e.g.,* Intuit at 4; NADA at 2; NIADA at 2, 4.

[35] Equifax at 2–4; Household at 1–2; NACAA at 1; NIADA at 4; SIIA at 2. *See also* NCHELP at 1.

[36] *See, e.g.,* Household at 1–2; NCHELP at 2; OCUL at 2; USA Funds at 1. *See also* Equifax at 2.

[37] Mastercard at 4–5. *See also* NRF at 4.

[38] NAMIC at 5–6.

[39] Equifax at 4.

[40] Ernst & Young at 1–2.

[41] Visa at 4.

[42] NIADA at 5.

[43] NIADA at 6 (but stating that the Rule's obligations for service providers are for the most part consistent with the Privacy Rule).

in disparate treatment of entities performing services for a bank and entities performing services for a financial institution under the FTC's jurisdiction. In addition, no commenters demonstrated that the confidentiality requirements that apply to auditors and accountants (or other professionals) would address unauthorized access to information by third parties, fraud, or any other security issues contemplated by the Rule. Further, given the Rule's flexibility, the Commission is aware of no duplicative burdens that will result from application of the Rule to auditors, accountants, or other professionals, or to service providers to, or affiliates of, banks. Finally, the Commission has determined that the Rule should apply to all service providers, even those that the Privacy Rule does not require to enter into agreements concerning reuse and redisclosure of the relevant information. Although the Privacy Rule allows certain service providers to receive information without entering into confidentiality agreements, these confidentiality provisions do not address the range of security issues that are contemplated by the Safeguards Rule.

Other comments sought minor clarifications of the definition of service provider. Specifically, commenters asked (1) whether a student loan organization is covered where the tasks it performs—passing along updated contact information to schools, lenders, loan servicers, and others involved in the funding of student loans—could not be carried out by financial institutions directly; [44] and (2) whether subservicers, employees and independent contractors of service providers are required to maintain separate safeguards.[45] These concerns are addressed as follows: First, although outsourcing often involves functions that may be performed in-house, the Commission sees no reason to exclude from the Rule service providers that are specifically authorized to perform services that a financial institution cannot perform itself. Thus, such entities are covered to the extent that they meet the definition. Second, the focus of the Rule's service provider provisions is clearly on the original service provider—the entity that provides services ''directly to a financial institution''— and not on subservicers or employees or independent contractors of these service providers. Although the original service provider should address the practices of these individuals and entities in its own security plan, the Rule does not specifically require these individual entities to maintain their own safeguards.

For the reasons discussed, the definition of service provider is adopted as proposed.

Section 314.3: Standards for Safeguarding Customer Information

Proposed paragraph (a) of this section set forth the general standard that a financial institution must meet to comply with the Rule, namely to ''develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards'' that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue. This standard is highly flexible, consistent with the comments, the Banking Agency Guidelines, and the Advisory Committee's Report, which concluded that a business should develop ''a program that has a continuous life cycle designed to meet the needs of a particular organization or industry.'' [46] *See* ACR at 18. Paragraph (a) also requires that each information security program include the basic elements set forth in proposed section 314.4 of the Rule, and be reasonably designed to meet the objectives set forth in section 314.3(b). For the reasons discussed below, this standard is adopted with only minor changes.

As noted above, commenters were generally supportive of the proposed standard, citing both its flexibility and its similarity to the Banking Agency Guidelines.[47] In addition, the numerous commenters who addressed whether the information security program should be in writing were supportive of this requirement,[48] stating that such a requirement is reasonable [49] and essential to the effective implementation and management of safeguards.[50] At the same time, two commenters suggested that the term ''comprehensive'' be deleted to avoid implying that the writing itself should be comprehensive.[51] One commenter urged that the Final Rule explicitly state—as was stated in the section-by-section analysis of the Proposed Rule [52]—that the writing need not be contained in a single document. In response, the Commission has amended the standard slightly, so that each financial institution must ''develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards'' that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue. *See* paragraph (a). The Commission believes that this standard will ensure a comprehensive, coordinated approach to security while emphasizing the flexibility of the writing requirement.

One commenter requested that the Rule specify that a financial institution need not disclose its information security plan to any third party other than law enforcers. In response, the Commission notes that the Rule itself creates no obligation for a financial institution to disclose its information security program. Moreover, the Privacy Rule requires a financial institution to disclose to consumers only the most general information about its safeguards. *See* 16 CFR 313.6(a)(8) and (c)(6). However, the Safeguards Rule leaves private parties free to negotiate disclosure of any safeguards information that may be relevant to the business at hand. Further, neither the G–L–B Act nor the Rule provides a shield to disclosure that is sought by law enforcement or pursuant to court order, subpoena or other legal process.

Section 314.4: Elements

This section sets forth the general elements that a financial institution must include in its information security program. The elements create a framework for developing, implementing, and maintaining the required safeguards, but leave each financial institution discretion to tailor its information security program to its own circumstances. Subject to the changes to paragraphs (d) and (e) that are set forth below, these elements are adopted as proposed.

1. Paragraph (a)

Paragraph (a) requires each financial institution to designate an employee or employees to coordinate its information security program in order to ensure accountability and achieve adequate safeguards. This requirement is similar to the Banking Agency Guidelines'

[44] TGSL at 2.

[45] Equifax at 4.

[46] The adaptability of the standard according to ''the sensitivity of information'' mirrors the Advisory Committee's finding that ''different types of data warrant different levels of protection.'' *Id.*

[47] *See supra* nn.15 and 16, and accompanying text.

[48] CDIA at 4; Equifax at 5; Intuit at 4; NFCU at 1; NFFG at 1; NCHELP at 3; NASAA at 2.

[49] *See, e.g.,* NCHELP at 3.

[50] *See, e.g.,* Intuit at 4.

[51] CDIA at 4; Equifax at 5.

[52] 66 FR at 41165.

requirement that each institution involve and report to its Board of Directors (*see* 66 FR 41166, *citing* Paragraphs III.A. and III.F., respectively), but allows designation of any employee or employees to better accommodate entities that are not controlled by Boards of Directors. Nearly all commenters on this paragraph expressed support, noting the importance of establishing a point of contact and citing the provision's flexibility.[53] However, some commenters requested minor changes, namely: (1) That the Rule state that a financial institution need not designate an employee for each of its subsidiaries; (2) that the words ''as appropriate'' be added to the requirement; and (3) that the Rule make clear that financial institutions may outsource safeguards procedures.[54] By contrast, one commenter opposed requiring financial institutions to designate any individual employee(s), based on a concern that customers might attempt to hold such designee(s) individually liable for any breach of security that occurs.[55]

The Commission recognizes the importance of reserving to financial institutions the flexibility to select and designate the employee(s) that are needed to ensure accountability and achieve adequate safeguards. The Commission is particularly concerned that small institutions not be burdened disproportionately by this paragraph (or by other requirements) of the Rule. For these reasons, the paragraph allows each financial institution to determine which employee(s) to designate, including whether to designate additional employees to handle different subsidiaries. Further, there is nothing in the Rule to prevent a financial institution from outsourcing safeguards functions as appropriate, provided that at least one of its own employees is designated to see that such functions are properly carried out. At the same time, the Commission declines to add the words ''as appropriate'' to this paragraph because such language would only repeat the Rule's overarching requirement that each financial institution develop, implement and maintain ''appropriate'' safeguards. Lastly, the Commission notes that this Rule does not address or alter traditional principles of corporate liability and, therefore, should neither create nor limit individual liability for a financial institution's designated employee(s). Thus, paragraph (a) is adopted as proposed.

2. Paragraph (b)

Proposed paragraph (b) required each financial institution to ''identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.'' The proposal further required each financial institution to consider risks in each area of its operations, including three areas that the Commission believes are particularly relevant to information security: (1) Employee training and management; (2) information systems, including information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures. This paragraph is similar to the Banking Agency Guidelines requirement to assess risks.[56]

Commenters who addressed the issue generally supported including a risk assessment requirement within the Rule.[57] Some of these commenters supported the paragraph as proposed, stating that its benefits are appropriate relative to its burdens, and that it provides the proper level of guidance on how risk assessment should be carried out.[58] Commenters that supported the paragraph's general description of the types of risks to be considered—including the proposed areas of operation—emphasized that the threats to information security are ever changing, and therefore can only be described in general terms.[59] By contrast, other commenters urged that the paragraph be made more specific in a variety of ways, namely by: (1) Defining specific categories of threats and hazards, such as ''risks to physical security;'' (2) including more concrete and extensive guidance on how small businesses might perform the required assessment; or (3) including a procedure by which the FTC will conduct reviews or audits of the security practices of financial institutions under its jurisdiction.[60]

The Commission notes the importance of providing guidance to financial institutions, particularly small businesses, on how to comply with this and other aspects of the Rule. The Commission therefore intends to issue educational materials to help businesses identify risks and comply with the various other provisions of the Rule. Because of the ever-changing nature of the relevant risks, however, the Commission does not find it appropriate to delineate risks more specifically within the Rule. In addition, to retain appropriate flexibility, the Commission will rely on its discretion in enforcing the Rule, and not describe any particular schedule or methods for enforcement.[61] At the same time, the Commission has amended slightly the areas of operation, in order to better describe the activities that financial institutions should consider in developing, implementing and maintaining their information security programs. Specifically, the Commission has added (1) the item ''network and software design'' to the examples of information systems a financial institution should examine; and (2) the term ''detecting'' to the requirement that each financial institution consider means of ''preventing and responding'' to attacks, intrusions and other systems failures. In all other respects, paragraph (b) is adopted as proposed.

3. Paragraph (c)

Proposed paragraph (c) required each financial institution to ''design and implement information safeguards to control the risks [identified] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.'' The proposal further required each financial institution to consider its areas of operation in fulfilling this requirement. As with proposed paragraph (b), above, commenters generally supported this provision, citing its flexibility and the appropriateness of its benefits relative to its burdens.[62] However, one commenter

[53] *See, e.g.,* Intuit at 4; Mastercard at 6–7; NACAA at 1–2; NCHELP at 3; Sallie Mae at 3; SIIA at 2; Visa at 2.

[54] Sallie Mae at 3; Equifax at 6; NRF at 5, respectively.

[55] NIADA at 6.

[56] *See* Banking Agency Guidelines, Paragraph III. B.

[57] *See, e.g.*, Equifax at 7; Intuit at 5; Mastercard at 7; NASAA at 2; NCHELP at 3; Portogo at 1; SIAA at 4; VeriSign at 1.

[58] *See, e.g.,* Intuit at 5; Mastercard at 7; SIAA at 2.

[59] Oracle at 2; Mastercard at 7.

[60] NACAA comment on the ANPR, at 2; Paas at 3; Musgrove at 2, respectively.

[61] By contrast to the Banking Agencies, the Commission is not authorized to conduct regular audits and review of entities under its jurisdiction.

[62] Intuit at 5; NCHELP at 4; SIIA at 2. In addition, as elsewhere, commenters urged that the paragraph include more guidance, so that businesses—particularly smaller entities, such as sole proprietorships—will better understand what safeguards are sufficient to comply with the Rule. *See* NIADA at 7–8; Paas at 4–5. As discussed above, the Commission agrees that educating businesses

Continued

asked that the provision be revised to require only such safeguards as are ''commercially reasonable,'' [63] while another urged that the paragraph require each financial institution to keep specific written records of its particular safeguards procedures, such as its employee training activities and records retention schedules, to demonstrate compliance with the Rule.[64]

The Commission recognizes that each financial institution must focus its limited resources on addressing those risks that are most relevant to its operations. However, because the Rule already contains flexible standards that take a variety of factors into account, the Commission does not believe it is necessary or appropriate to revise the Rule to require only such safeguards as are ''commercially reasonable.'' At the same time, to preserve flexibility and minimize burdens, the Commission declines to revise this paragraph to require that financial institutions document specific aspects of their risk control activities. For these reasons, paragraph (c) is adopted as proposed.

4. Paragraph (d)

Proposed paragraph (d) required each financial institution to oversee its service providers by selecting and retaining service providers that are ''capable of maintaining appropriate safeguards'' for the customer information at issue (paragraph (d)(1)), and requiring its service providers by contract to ''implement and maintain such safeguards'' (paragraph(d)(2)). For the reasons discussed below, paragraph (d)(1) is revised slightly, while paragraph (d)(2) is adopted as proposed.

Commenters supported requiring oversight of service providers' safeguards by financial institutions, particularly when, as one coalition of financial services organizations noted, the financial services industry increasingly relies on third parties to support core functions and online delivery.[65] However, in commenting on proposed paragraph (d)(1), some commenters expressed concern about the ability of businesses—particularly smaller entities—to evaluate a service provider's capabilities.[66] At the same time, other commenters supported adding to the Rule various standards for financial institutions to use in selecting service providers, specifically: (1) That financial institutions have ''reason to believe'' their service providers are capable of maintaining appropriate safeguards; [67] (2) that they use a ''due diligence'' review, as under the Banking Agency guidelines; [68] or (3) that they select service providers that are ''capable of maintaining appropriate safeguards.'' [69]

The Commission agrees that businesses cannot be expected to perform unlimited evaluation of their service providers' capabilities. Thus, the Commission has amended the provision to state that each financial institution must ''take reasonable steps'' to select and retain appropriate service providers. This added language more closely parallels the Banking Agency Guidelines, as well as the Rule's requirement to assess risks that are ''reasonably foreseeable.'' The steps that are reasonable under the Rule will depend upon the circumstances and the relationship between the financial institution and the service provider in question. At a minimum, the Commission envisions that each financial institution will (1) take reasonable steps to assure itself that its current and potential service providers maintain sufficient procedures to detect and respond to security breaches, and (2) maintain reasonable procedures to discover and respond to widely-known security failures by its current and potential service providers.

Proposed paragraph (d)(2) required financial institutions to enter into contracts that require service providers to implement and maintain appropriate safeguards. Most comments that addressed this requirement supported it.[70] Nevertheless, as discussed above, some commenters urged that certain service providers be exempt from the Rule, or be permitted to comply with the safeguards standards of another agency, such as their own functional regulator in the case of financial institution service providers. These comments already have been addressed above. In addition, two commenters urged that the Rule give examples of appropriate language or specifically require the inclusion of certain clauses in the contract,[71] while other commenters stated that no such specifications are needed or desirable.[72] The Commission believes that financial institutions are well positioned to develop and implement appropriate contracts with their service providers. Further, keeping the contract provision flexible should allow financial institutions and their service providers to develop arrangements that do not impose undue or conflicting burdens on service providers that may be subject to other standards and/or agreements concerning safeguards. Therefore, the Commission declines to include specific contract language within the Rule. However, the Commission intends to provide education for businesses on how to comply with the Rule, and will include general guidance concerning oversight of service providers as part of this effort. For these reasons, paragraph (d)(2) is adopted as proposed.

5. Paragraph (e)

Proposed paragraph (e) required each financial institution to ''evaluate and adjust [its] information security program in light of any material changes to [its] business that may affect [its] safeguards.'' The preamble to the proposed section offered examples of such material changes, namely changes in technology; changes to its operations or business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, or changes to the services provided; new or emerging internal or external threats to information security; or any other circumstances that give it reason to know that its information security program is vulnerable to attack or compromise. *See* 66 FR 41167. Several commenters supported this requirement as proposed.[73] However, a few commenters recommended certain revisions to the paragraph's description of the types of changes that may warrant evaluation and adjustment of an entity's safeguards. Specifically, one commenter urged that although changes in the sensitivity of customer information or the nature of any threats will warrant evaluation, changes to a business's internal organization may be irrelevant to its safeguards, and therefore should not necessitate a review.[74] Similarly, another commenter urged that the paragraph be revised to require that a financial institution ''take reasonable steps so that the information security

and others is critical to achieving the Rule's objectives, and plans to issue educational materials in connection with the Rule.

[63] Equifax at 8.

[64] Musgrove at 2.

[65] BITS at 1. *See also* CDIA at 6; ITAA at 3; VeriSign at 2 (Rule appropriately places on financial institutions the burden to select appropriate service providers).

[66] Paas at 5. *See also* NRF at 5 (expressing concern that Rule could make financial institutions strictly liable for safeguards breaches by their service providers).

[67] NRF at 5; TGSL at 2.

[68] Household at 1; ICBA at 1; NIADA at 6.

[69] Mastercard at 7.

[70] Equifax at 8; Indep. Ins. Agents 3; Intuit at 5; Mastercard at 7; NACAA at 2; NCHELP at 4; Navy Federal Financial Group at 1–2; NIADA at 7; Sallie Mae at 3; SIIA at 2.

[71] NADA at 3; Navy Federal Financial Group at 1–2.

[72] Intuit at 5; Sallie Mae at 3.

[73] NACAA at 2; NCHELP at 5; SIIA at 2.

[74] Intuit at 6.

program continues to be appropriate'' for the financial institution.[75]

Consistent with the intent of the Proposed Rule, as well as the concerns reflected in these comments, the Commission believes that the bases for a financial institution to adjust its information security program will vary depending on the circumstances and may include a wide range of factors. Accordingly, paragraph (e) has been amended to more clearly reflect the fact-specific nature of the inquiry and to better encompass the broad range of factors that a financial institution should consider. Under the revised paragraph, each financial institution must evaluate and adjust its information security program ''in light of the results of the testing and monitoring required by paragraph (c); any material changes to [its] operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on [its] information security program.'' The Commission believes that the Rule allows a financial institution sufficient flexibility as to how to adjust its safeguards, and therefore finds it unnecessary to limit the responsibility of financial institutions to taking ''reasonable steps'' to make any adjustments. Thus, paragraph (e) is adopted with the changes noted above.

Section 314.5: Effective Date

Proposed section 314.5 required each financial institution covered by the Rule to implement an information security program not later than one year from the date on which a Final Rule is issued. In addition, the proposal requested comment on whether the Rule should contain a transition period to allow the continuation of existing contracts with service providers, even if the contracts would not satisfy the Rule's requirements.

Many commenters supported as adequate an effective date of one year from the date on which the Final Rule is issued.[76] A few commenters urged that a longer time be given, such as 18 months,[77] or that an additional year be allowed for businesses—particularly small entities—to comply.[78] In addition, all commenters who addressed the issue urged that the Rule allow a transition period for service provider contracts.[79] Most of these commenters requested that financial institutions be given two years to make service provider contracts comply,[80] while a few commenters sought a slightly longer time.[81]

Consistent with the majority of comments, the Rule will take effect one year from the date on which the Final Rule is published in the **Federal Register**, except that there will be a transition rule for contracts between financial institutions and nonaffiliated third party service providers. Under the transition Rule, set forth in section 314.5(b) of the Rule, financial institutions will be given an additional year to bring these service provider contracts into compliance with the Rule, as long as the contract was in place 30 days after the date on which the Final Rule is published in the **Federal Register**. The transition rule parallels the two-year grandfathering of service contracts that was permitted under both the Privacy Rule and the Banking Agency Guidelines. The Commission believes that the effective date and transition rule will provide businesses appropriate flexibility in complying with the Rule.

Section D. Paperwork Reduction Act

The Paperwork Reduction Act (''PRA''), 44 U.S.C. Chapter 35, requires federal agencies to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons. 44 U.S.C. 3502(3)(a)(i). Under the PRA, a rule creates a ''collection of information'' where ten or more persons are asked to report, provide, disclose, or record information'' in response to ''identical questions.'' *See* 44 U.S.C. 3502(3)(A). Applying these standards, the Rule does not constitute a ''collection of information.'' The Rule calls upon affected financial institutions to develop or strengthen their information security programs in order to provide reasonable safeguards. Under the Rule, each financial institution's safeguards will vary according to its size and complexity, the nature and scope of its activities, and the sensitivity of the information involved. For example, a financial institution with numerous employees would develop and implement employee training and management procedures beyond those that would be appropriate or reasonable for a sole proprietorship, such as an individual tax preparer or mortgage broker. Similarly, a financial institution that shares customer information with numerous affiliates would need to take steps to ensure that such information remains protected, while a financial institution with no affiliates would not need to address this issue. Thus, although each financial institution must summarize its compliance efforts in one or more written documents, the discretionary balancing of factors and circumstances that the Rule allows—including the myriad operational differences among businesses that it contemplated—does not require entities to answer ''identical questions,'' and therefore does not trigger the PRA's requirements. *See* ''The Paperwork Reduction Act of 1995: Implementing Guidance for OMB Review of Agency Information Collection,'' Office of Information and Regulatory Affairs, OMB (August 16, 1999), at 20–21.

Section E. Regulatory Flexibility Act

In its ANPR, the Commission stated its belief that, under the Regulatory Flexibility Act (''RFA''), 5 U.S.C. 604(a), it was not required to issue an Initial Regulatory Flexibility Analysis (''IRFA'') because the Commission did not expect that the Proposed Rule would have a significant economic impact on a substantial number of small entities within the meaning of the Act. *See* 66 FR at 41167. The Commission nonetheless issued an IRFA with the Proposed Rule in order to inquire into the possible impact of the Proposed Rule on small entities, and to provide information to small businesses, as well as other businesses, on how to implement the Rule. *Id.*

Although the Commission specifically sought comment on the costs to small entities of complying with the Rule, no commenters provided specific cost information. Some commenters generally praised the proposal's flexibility[82] or noted that given its flexible standards, it was appropriate for the Rule to apply equally to businesses of all sizes.[83] However, other commenters suggested that small entities may be disproportionately burdened by the Rule because they lack expertise (relative to larger entities) in developing, implementing and maintaining the required safeguards.[84] In light of these comments, the Commission has carefully considered whether to certify that the Rule will not have a significant impact on a

[75] Equifax at 9.

[76] *See, e.g.*, Equifax at 10; Intuit at 6; Mastercard at 8; NIADA at 8; OCUL at 3; Sallie Mae at 3; SIIA at 2; USA Funds at 1–2.

[77] NADA at 2–3; NIADA at 8. *See also* NFFG at 2 (2 years).

[78] ACA at 6–7.

[79] *See, e.g.*, CDIA at 5; NIADA at 8; OCUL at 3; SIIA at 2; TGSL at 2; Visa at 5.

[80] *See, e.g.*, Equifax at 10; NRF at 5; NFFG at 2; OCUL at 3.

[81] Sallie Mae at 3; Visa at 5.

[82] *See, e.g.*, Household at 1; SIIA at 1; TGSL at 1; VeriSign at 1.

[83] Intuit at 2; NASAA at 2.

[84] *See, e.g.*, NADA at 2; NIADA at 9; Musgrove at 2 (stating that small financial institutions may need to hire outside consultants to comply with Rule).

substantial number of small entities. The Commission continues to believe that the Rule's impact will not be substantial in the case of most small entities. However, the Commission cannot quantify the impact the Rule will have on such entities. Therefore, in the interest of thoroughness, the Commission has prepared the following Final Regulatory Flexibility Analysis (''FRFA'') with this Final Rule. 5 U.S.C. 605.

1. Succinct Statement of the Need for, and Objectives of, the Rule

The Final Rule is necessary in order to implement section 501(b) of the G–L–B Act, which requires the FTC to establish standards for financial institutions subject to its jurisdiction relating to administrative, technical, and physical standards. According to section 501(b), these standards must: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. These objectives have been discussed above in the statement of basis and purpose for the Final Rule.

2. Summary of the Significant Issues Raised by the Public Comments in Response to the IRFA; Summary of the Assessment of the Agency of Such Issues; and Statement of Any Changes Made in the Rule as a Result of Such Comments

As stated above, no comments were received concerning specific costs that will be imposed on small entities by the Rule. However, some commenters stated that the Rule and/or certain of its requirements would impose high costs on businesses, including small entities.[85] In addition, as stated, a few commenters suggested that small entities may be disproportionately burdened by the Rule because they lack expertise (relative to larger entities) in developing, implementing and maintaining the required safeguards.[86] Finally, as stated above, many commenters urged that the Commission provide guidance on how to comply with the Rule to assist entities—particularly smaller businesses—to comply without incurring undue expense.[87] In addition, some commenters specifically requested guidance on how to assess risks as required by section 314.4(b);[88] develop, implement and maintain safeguards as required by section 314.4(c); [89] and oversee service providers as required by section 314.4(d).

The Commission took comments respecting the Rule's impact on small entities into account by designing flexible safeguards standards (section 313.3(a)). Similarly, the Commission took smaller entities into account in allowing each financial institution to decide for itself what employees to designate to handle safeguards (section 314.4(a)), in order to give businesses, particularly smaller entities, flexibility in complying with the Rule. Lastly, because some commenters expressed concern about the ability of businesses—particularly smaller entities—to evaluate a service provider's capabilities,[90] the Commission amended the relevant paragraph to state that each financial institution must ''take reasonable steps'' to select and retain appropriate service providers.

In addition to the above changes, the Commission has taken into account those comments that stated the importance of educating businesses and others on how to implement and maintain information safeguards. The Commission agrees that such education is critical to achieving the Rule's objectives and to minimizing burdens on businesses. Thus, as stated in the Rule's preamble, the Commission plans to provide educational materials on or near the date on which compliance is required. As part of this effort, the Commission intends to perform outreach to inform small entities, such as individual tax preparers or other sole proprietors, of the Rule and its requirements.

In addition to the forthcoming educational materials, the Commission has given guidance in the Rule and its Preamble that is intended to assist businesses, particularly small entities, to comply with the Rule. Specifically, as discussed above, the Commission has included within the Rule a brief description of those areas of a business' operations that the Commission believes are most relevant to information security: (1) Employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures. *See* section 314.3(b).

3. Description and Estimate of the Number of Small Entities to Which the Rule Will Apply or an Explanation of Why No Such Estimate Is Available

As previously discussed in the IRFA accompanying the Proposed Rule, it is difficult to estimate accurately the number of small entities that are financial institutions subject to the Rule. The definition of ''financial institution,'' as under the Privacy Rule, includes any institution the business of which is engaging in a financial activity, as described in section 4(k) of the Bank Holding Company Act, which incorporates by reference the activities listed in 12 CFR 225.28 and 12 CFR 211.5(d), consolidated in 12 CFR 225.86. *See* 65 FR 14433 (Mar. 17, 2000).

The G–L–B Act does not specify the categories of financial institutions subject to the Commission's jurisdiction; rather, section 505(a)(5) vests the Commission with enforcement authority with respect to ''any other financial institution or other person that is not subject to the jurisdiction of any [other] agency or authority [charged with enforcing the statute].'' Financial institutions covered by the Rule will include many of the same lenders, financial advisors, loan brokers and servicers, collection agencies, financial advisors, tax preparers, real estate settlement services, and others that are subject to the Privacy Rule. Many of these financial institutions will not be subject to the Safeguards Rule to the extent that they do not have any ''customer information'' within the meaning of the Safeguards Rule. The Commission did not receive comments that helped it to identify in any comprehensive manner the small entities that will be affected by the rule. However, one commenter, the National Association of Automobile Dealers Association (''NADA'') submitted 1999 data showing that, at that time, 5,292 franchised new automobile dealers had 30 or fewer employees; 1,706 had 20 or fewer employees; and 575 had 10 or fewer employees.[91] In addition, the Commission is aware that many small businesses, such as individual tax preparers or mortgage brokers, will be covered by the Rule.

[85] FPA at 3; Paas at 2; *see also* OCUL (stating that the NCUA's safeguards rule is very burdensome for credit unions); Post at 1 (stating that Privacy Rule is very burdensome).

[86] *See supra* n. 81.

[87] *See, e.g.,* ICB at 2; Musgrove at 2; NADA at 2; NIADA at 9; Paas at 4–6.

[88] Paas at 3.

[89] *See* NIADA at 7; Paas at 4–5.

[90] Paas at 5; *see also* NRF at 5 (expressing concern that Rule could make financial institutions strictly liable for safeguards breaches by their service providers).

[91] NADA at 1.

4. Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Rule, Including an Estimate of the Classes of Small Entities That Will Be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record

As explained in the Commission's IRFA and the Paperwork Reduction Act discussion that appears elsewhere in this document, the Safeguards Rule does not impose any specific reporting or recordkeeping requirements. Accordingly, compliance with the Rule does not entail expenditures for particular types of professional skills that might be needed for the preparation of such reports or records.

The Rule, however, requires each covered institution to develop a written information security program covering customer information that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. The institution must designate an employee or employees to coordinate its safeguards; identify reasonably foreseeable risks and assess the effectiveness of any existing safeguards for controlling these risks; design and implement a safeguards program and regularly monitor its effectiveness; require service providers (by contract) to implement appropriate safeguards for the customer information at issue; and evaluate and adjust its program to material changes that may affect its safeguards, such as new or emerging threats to information security. As discussed above, these requirements will apply to institutions of all sizes that are subject to the FTC's jurisdiction pursuant to the Rule, including small entities, although the Commission did not receive comments that would enable a reliable estimate of the number of such small entities.

In light of concerns that compliance with these requirements might require the use of professional consulting skills that could be costly, the Commission, as explained in its IRFA, fashioned the Rule's requirements to be as flexible as possible consistent with the purposes of the G–L–B Act, so that entities subject to the Rule, including small entities, could simplify their information security program to the same extent that their overall operations are simplified. Furthermore, the Commission invited comments on the costs of establishing and operating an information security program for such entities, particularly any costs stemming from the proposed requirements to: (1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, and (2) develop a comprehensive information security program in written form. In response to comments that raised concerns that many businesses would not possess the required resources or expertise to fulfill the Rule's requirements, the Commission notes that the Rule is not intended to require that entities hire outside experts or consultants in order to comply. Further, the Commission has noted that it intends to provide educational materials that will assist such entities in compliance. In addition, in response to concerns that the preparation of a written plan could be burdensome, the Commission amended this requirement slightly to emphasize the flexibility of the writing requirement and make clear that the writing need not be contained in a single document.

5. Description of the Steps the Agency Has Taken To Minimize the Significant Economic Impact on Small Entities, Consistent with the Stated Objectives of Applicable Statutes, Including a Statement of the Factual, Policy, and Legal Reasons for Selecting the Alternative Adopted in the Final Rule and Why Each of the Other Significant Alternatives to the Rule Considered by the Agency That Affect the Impact on Small Entities Was Rejected

The G–L–B Act requires the FTC to issue a rule that establishes standards for safeguarding customer information. The G–L–B Act requires that standards be developed for institutions of all sizes. Therefore, the Rule applies equally to entities with assets of $100 million or less, and not just to larger entities.

As previously noted, the Commission does not believe the Safeguards Rule imposes a significant economic impact on a substantial number of small entities. Nonetheless, to the extent that small entities are subject to the Rule, it imposes flexible standards that allow each institution to develop an information security program that is appropriate to its size and the nature of its operations. In this way, the impact of the Rule on small entities and any other entities subject to the Rule is no greater than necessary to effectuate the purposes and objectives of the G–L–B Act, which requires that the Commission adopt a rule specifying procedures sufficient to safeguard the privacy of customer information protected under the Act. To the extent that commenters suggested alternative regulatory approaches—such as that compliance with alternative standards be deemed compliance with the Rule—that could affect the Rule's impact on small entities, those comments and the Commission's responses are discussed above in the statement of basis and purpose for the Final Rule.

List of Subjects for 16 CFR Part 314

Consumer protection, Credit, Data protection, Privacy, Trade practices.

Final Rule

For the reasons set forth in the preamble, the Federal Trade Commission amends 16 CFR chapter I, subchapter C, by adding a new part 314 to read as follows:

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.

Authority: 15 U.S.C. 6801(b), 6805(b)(2).

§ 314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (''FTC'' or ''Commission'') has jurisdiction. This part refers to such entities as ''you.'' This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§ 314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure 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.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

§ 314.5 Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 02–12952 Filed 5–22–02; 8:45 am]

BILLING CODE 6750–01–P