persons and organizations. In addition, the update is available on line through the FSIS web page at *http://www.fsis.usda.gov.* The update is used to provide information regarding FSIS policies, procedures, regulations, **Federal Register** notices, FSIS meetings, recalls, and any other types of information that could affect or would be of interest to our constituents/shareholders. The constituent fax list consists of industry, trade, and farm groups, consumer interest groups, allied health professionals, scientific professionals, and others who have requested to be included. Through these various channels, FSIS is able to provide information to a much broader, more diverse audience. For more information and to be added to the constituent fax list, fax your request to the Congressional and Public Affairs Office at (202) 720–5704.

Done in Washington, DC, on: August 2, 2001.

Thomas J. Billy,

Administrator.

[FR Doc. 01–19749 Filed 8–6–01; 8:45 am]

BILLING CODE 3410–DM–P

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084 AA87

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Proposed rule; request for public comment.

SUMMARY: The Federal Trade Commission (''FTC'' or ''Commission'') is proposing certain standards relating to administrative, technical, and physical information safeguards for financial institutions subject to the Commission's jurisdiction. The Gramm-Leach-Bliley Act (''G–L–B Act'' or ''Act'') requires the Commission to issue these standards. They are intended to: insure 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.

DATES: Comments must be received not later than October 9, 2001.

ADDRESSES: Written comments should be addressed to: Secretary, Federal Trade Commission, Room 159, 600 Pennsylvania Avenue, NW., Washington, DC 20580. The Commission requests that commenters submit the original plus five copies, if feasible. All comments will be posted on the Commission's Web site: *www.ftc.gov.* To enable prompt review and public access, paper submissions should include a version on diskette in PDF, ASCII, WordPerfect or Microsoft Word format. Diskettes should be labeled with: (1) The name of the commenter and (2) the name and version of the word processing program used to create the document. Alternatively, documents may be submitted to the following email address: *GLB501Rule@ftc.gov.* Parties submitting comments via email should (1) confirm receipt by consulting the postings on the Commission's Web site, *www.ftc.gov;* and (2) indicate whether they are also providing their comments in other formats. Individual members of the public filing comments need not submit multiple copies or comments in electronic form. All submissions should be captioned ''Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 CFR Part 314—Comment.''

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:

A. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Public Law 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. Under the Act, banks are now permitted to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities.

Title V of the Act, captioned ''Disclosure of Nonpublic Personal Information,'' addresses privacy and security issues raised by these new arrangements and covers a broad range of traditional and non-traditional financial institutions. Regarding privacy, the Act limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties; it also requires a financial institution to make certain disclosures concerning its privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. *See* sections 502 and 503, respectively. 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 is required on or before July 1, 2001.

Regarding the security of financial information, the Act requires the Commission and certain other federal agencies (''the Agencies'') to establish standards for financial institutions relating to administrative, technical, and physical information safeguards.[2] *See* 15 U.S.C. 6801(b), 6805(b)(2). As described in the Act, the objectives of these standards are to: (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. *See* 15 U.S.C. 6801(b) (1)–(3). While 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.[3]

On September 7, 2000, the Commission published in the **Federal Register** a Notice and Request for Comment (''the Notice'') on the scope and potential requirements of a Safeguards Rule for the financial institutions subject to its jurisdiction. 65 FR 54186. The Comment period for the Notice ended on October 24, 2000, and the Commission received 30 comments

[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''). In addition, on December 21, 2000, Congress amended the Commodity Exchange Act to add the Commodity Futures Trading Commission (''CFTC'') to the list of federal functional regulators.

[3] Although section 504 of the Act required the Agencies to work together to issue consistent and comparable rules to implement the Act's privacy provisions, the Act does not require the Agencies to coordinate in developing their safeguards standards. Where appropriate, however, the Commission has sought consistency with the other agencies' standards, particularly those issued by the banking agencies (see n.5, *infra*).

from a variety of interested parties.[4] The Commission has considered those comments, as well as the standards adopted by the other Agencies, in formulating its proposed rule.[5] The Commission also has considered the Final Report that was issued by the Federal Trade Commission Advisory Committee on Online Access and Security on May 15, 2000 (hereinafter ''Advisory Committee's Report'' or ''ACR'').[6] While the Advisory Committee's Report addressed security only in the online context, the Commission believes that its principles have general relevance to information safeguards. The Commission now offers for comment a proposed rule governing the safeguarding of customer records and information for the financial institutions subject to its jurisdiction.

B. Overview of Comments Received

As noted above, the Notice sought comment on the potential scope and requirements of a Commission rule, including the proper level of specificity of the rule's requirements,[7] and the extent to which the rule should resemble the other Agencies' standards. 65 FR at 54189. Of the 30 comments the Commission received,[8] three were from corporations or associations related to higher education or the funding of student loans; [9] seven were from corporations performing various financial or internet-related services; [10] two were from companies that provide information security services; [11] seven were from trade associations; [12] one was from a non-profit association of consumer groups; [13] three were from other governmental or non-profit professional associations; [14] and six were from individuals and other interested parties.[15] Virtually all of the comments urged that the standards for safeguarding information be flexible, and contain few, if any, specific requirements.[16] These comments pointed out that institutions need discretion to make decisions appropriate to their current operations and to adapt to changes in technology and their business environments,[17] and that implementation of the rule should not disrupt safeguards programs that entities have in place already.[18] In addition, many private companies praised the flexibility of the then-proposed guidelines issued by the banking agencies (''Banking Agency Guidelines''), and stated that conforming the Commission's rule to the Guidelines would minimize the burden of complying with the rule.[19]

These comments were instrumental in shaping the proposed rule. In particular, consistent with the majority of comments, the proposed rule follows the general approach of the Banking Agency Guidelines, and contains flexible requirements wherever feasible. To ensure flexibility, the proposed rule provides that each information security program should be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of the customer information at issue.[20] At the same time, consistent with the Banking Agency Guidelines, the proposed rule requires that certain basic elements that the Commission believes are important to information security be included in each program. Thus, each financial institution must: (1) Designate an employee or employees to coordinate its program; (2) assess risks in each area of its operations; (3) design and implement an information security program to control these risks; (4) require service providers (by contract) to implement appropriate safeguards for the customer information at issue; and (5) adapt its program in light of material changes to its business that may affect its safeguards. These elements create a general procedural framework, so that each financial institution can develop, implement, and maintain appropriate safeguards even as its circumstances change over time.

Comments respecting the impact of the Safeguards Rule on small entities also were important in developing the proposed rule. Some commenters pointed out that making the rule's requirements flexible would enable smaller institutions to implement appropriate programs without setting too low a target for more sophisticated operations.[21] The proposed standard described above, which explicitly allows for flexibility according to the size and complexity of a financial institution and the nature and scope of its activities, should minimize the rule's burdens on small entities.

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

C. Section-by-Section Analysis

The Commission proposes to issue the Safeguards Rule as a new 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 proposed rule.

[4] In response to a request from a commenter, the Commission added 14 days to the initial 30-day comment period. 65 FR 59766 (Oct. 6, 2000).

[5] Since publication of the Notice, the NCUA and the remaining banking agencies—the OCC, the Board, the FDIC, and OTS—have issued final guidelines. 66 FR 8152 (Jan. 30, 2001); 66 FR 8616 (Feb. 1, 2001). Earlier, on June 29, 2000, the SEC had adopted a final safeguards rule as part of its Privacy of Consumer Financial Information Final Rule (hereinafter ''SEC rule''). 65 FR 40334. On March 21, 2001, the CFTC issued a proposed rule that mirrors the SEC rule. *See* 66 FR 15550 at 15562, 15574. As with the Privacy Rule, Treasury will not be issuing a separate rule.

[6] The Advisory Committee was composed of 40 members (including representatives from industry, consumer groups, and academia) nominated through a public notice and comment process. *See* 64 FR 71457 (Dec. 21, 1999). One of its main purposes was to give advice and recommendations to the Commission regarding the implementation of adequate security for personal information collected from consumers online. ACR at 2. Its charter, membership, and Report are available on the Commission's website, at *www.ftc.gov.*

[7] Among other things, it asked whether the rule should set forth particular minimum procedures a financial institution must follow, or should rely on more general standards, such as ''reasonable policies and procedures'' to achieve the Act's purposes. 65 FR at 54188.

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

[9] Iowa Student Loan Liquidity Corporation (''Iowa Student Loan''); Texas Guaranteed Student Loan Corp. (''TGSL''); United Student Aid Funds, Inc. (''USA Funds'').

[10] Household Finance Corporation (''Household''); Intuit; MasterCard International (''MasterCard''); Morgan Stanley Dean Witter Credit Corporation (''MSDWCC''); Plainview Financial Services, Ltd. (''Plainview''); Visa USA, Inc. (''Visa''); 724 Solutions, Inc. (''724 Solutions'').

[11] RSA Security, Inc.; Tiger Testing.

[12] American Collectors Ass'n, Inc. (''ACA''); America's Community Bankers (''ACB''); Credit Union Nat'l Ass'n (''CUNA''); Nat'l Ass'n of Indep. Insurers (''NAII''); Nat'l Indep. Automobile Dealers Ass'n (''NIADA''); Nat'l Council of Investigation and Security Services, Inc. (''NCISS''); Nat'l Retail Federation (''NRF'').

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

[14] Committee on Internet and Litigation of the Commercial and Federal Litigation Section, New York State Bar Ass'n (CI & L); Nat'l Ass'n of Attorneys General (''NAAG''); North American Securities Administrators Ass'n, Inc. (''NASAA'').

[15] Calvin Ashley (''Ashley''); Professor Mark Budnitz, Georgia State Univ. College of Law; Evan Hendricks, Editor/Publisher of *Privacy Times,* and Consultant to PrivaSys; John Merryman; Martin D. Rosenblatt, MD; Doug Scala.

[16] ACA at 5; ACB at 1; CI & L at 2; Household at 1; Intuit at 2, 4, 6; Iowa Student Loan at 1; MasterCard at 2, 3; NIADA at 1, 3; TGSL at 1; USA Funds at 3; Visa at 2.

[17] *See, e.g.,* Intuit at 2; NRF at 5; Visa at 2.

[18] *See, e.g.,* CI & L at 2; Intuit at 5–6; Iowa Student Loan at 1.

[19] *See, e.g.,* Intuit at 14; USA Funds at 6; Visa at 1–2, 4.

[20] This approach is also constituent with the Advisory Committee's finding, in the online context, that security is ''contextual'' and that a security program should have a ''continuous life cycle designed to meet the needs of the particular organization or industry.'' *See* ACR at 18.

[21] ACB at 4; *see also* ACA at 5; Plainview at 2.

Proposed section 314.1: Purpose and Scope

Paragraph 314.1(a) sets forth the general purpose of the proposed rule, which is 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.

Paragraph 314.1(b) sets forth the scope of the proposed rule, which applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction. As noted in the Privacy Rule, covered financial institutions include: non-depository lenders, consumer reporting agencies, 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 other entities under the Commission's jurisdiction that are significantly engaged in financial activities.[22] As proposed, the rule covers the handling of customer information by all financial institutions under the Commission's jurisdiction, including not only financial institutions that collect information from their own customers, but also financial institutions that receive customer information from other financial institutions.[23] Although comments were mixed on this point,[24] the Commission believes that including recipient financial institutions within the rule will assure greater safeguards for customer information and is within the authority conferred by the Act. Nevertheless, the Commission requests comment on the benefits and burdens of this requirement and/or other issues or concerns that it raises.

Recipients of customer information that are not financial institutions are not directly subject to the proposed rule's requirements. However, as discussed in greater detail below, the proposed rule requires financial institutions to ensure that customer information remains protected when it is shared with their affiliates and service providers, some of which may not be financial institutions. *See* proposed paragraph 314.2 (b) (defining ''customer information'' to include information handled or maintained by or on behalf of affiliates); proposed paragraph 314.5(d) (requiring a financial institution to select and retain appropriate service providers, and to enter into contracts requiring them to maintain appropriate safeguards).[25] As discussed below, the Commission is seeking comment on the various issues raised by these proposed provisions.

A few commenters urged that compliance with alternative standards should constitute compliance with the Safeguards Rule. For example, one commenter urged that compliance with the SEC rule should 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 covered by the SEC rule.[26] Similarly, another commenter urged that compliance with the Family Educational Rights and Privacy Act (''FERPA'') should satisfy the Safeguards Rule, just as it satisfies the Privacy Rule.[27] The comment explained that FERPA protects the security and integrity of student records by a variety of requirements, including mandatory written student consent prior to the release of personally identifiable information.[28] The Commission requests additional comment on whether and how compliance with these and other laws and rules relating to information security—including the rules relating to medical information under the Health Insurance Portability and Accountability Act (''HIPAA'') of 1996—should be addressed in the proposed rule.

Proposed section 314.2: Definitions

This section defines terms for purposes of the proposed Safeguards Rule. Proposed paragraph (a) of this section makes clear that, unless otherwise stated, terms used in the Safeguards Rule bear the same meaning as in the Commission's Privacy Rule. Thus, for example, ''customer'' under the Safeguards Rule is the same as under the Privacy Rule: a consumer who has established a continuing relationship with an institution.[29] 16 CFR 313.3(h). Further, ''affiliate'' means ''any company that controls, is controlled by, or is under common control with another company.'' 16 CFR 313.3(a).[30] The proposed Safeguards Rule also defines the following new terms: ''customer information;'' ''information security program;'' and ''service provider.'' *See* paragraphs (b), (c), and (d), respectively, of proposed section 314.2.

Proposed paragraph (b) defines ''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.[31] The Commission proposes to include information handled or maintained by or on behalf of affiliates in this definition to ensure that customer information does not lose its protections merely because it is shared with affiliates, which is freely allowed under the G–L–B Act and Privacy Rule.[32] Thus, to the extent that a financial institution shares customer information with its affiliates, the proposed rule would require it to ensure that the affiliates maintain appropriate safeguards for the customer information at issue.

---

[22] 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.

[23] Such recipient entities might include service providers or affiliates of financial institutions that are also financial institutions themselves. They might also include entities such as consumer reporting agencies that routinely receive customer information from other financial institutions.

[24] Some commenters stated that the rule should establish safeguards only for a financial institution's handling of information about its own customers, and not for such information in the hands of third-party financial institutions. *See, e.g.,* ACA at 4; MasterCard at 4. By contrast, others urged that, consistent with the way that the Privacy Rule's restrictions remain affixed to information when it is disclosed by a financial institution, safeguards should not be lost when information is transferred to another financial institution. NAAG at 2; *see also* Intuit at 3–4, 13; NIADA at 2; USA Funds at 1.

[25] Although the proposed rule does not impose duties on financial institutions with respect to other recipients of information, the Commission notes that financial institutions must also comply with the Privacy Rule, as well as section 5 of the FTC Act, which prohibits unfair or deceptive acts and practices. Therefore, financial institutions must ensure that any statements they make regarding the security of customer information or the manner in which it is handled by third parties must be accurate.

[26] NASAA at 2.

[27] ACE at 1–2.

[28] *Id.* at 2–3; *see also* USA Funds.

[29] By virtue of the Privacy Rule's definition of ''consumer,'' customer does not include a business. *See* sections 313.3(e) and (h) of the Privacy Rule (defining ''consumer'' and ''customer,'' respectively).

[30] Other relevant definitions from the Privacy Rule include: ''control,'' ''nonpublic personal information,'' and as discussed above, ''financial institution.'' *See* 16 CFR 313.3(g), (n), and (k), respectively.

[31] Section 501(b) of the Act refers to the protection of both customer ''records'' and ''information.'' However, for the sake of simplicity, the proposed rule (like the Banking Agency Guidelines) uses the term ''customer information'' to encompass both information and records.

[32] *See* section 502(a) (restricting disclosures only to nonaffiliated third parties).

The Commission recognizes that certain entities (*e.g.*, banks) that meet the proposed rule's definition of ''affiliate'' simultaneously may be covered by another agency's safeguards standards. In response, the Commission notes that it does not intend to duplicate existing requirements for affiliates that are financial institutions directly subject to safeguards standards. Instead, the proposed requirement is designed to ensure that safeguards are not lost in the event that customer information is disclosed to an affiliate that is not a financial institution, or that is not required to safeguard information about another financial institution's customers. The Commission requests comment on: (1) The benefits and burdens of this proposal, including any compliance burdens imposed on entities already covered by the safeguards standards of other Agencies; (2) whether any additional guidance is needed on what safeguards are appropriate for affiliates; and (3) other issues or concerns raised by this requirement. The Commission also requests comment on whether information shared with affiliates already is protected adequately by other provisions of the proposed rule.[33]

The proposed Safeguards Rule applies solely to ''customer information'' and not to information about other consumers who do not meet the definition of ''customer.'' This approach is consistent with the Banking Agency Guidelines, as well as the majority of comments that addressed this issue.[34] The commenters pointed out that the language of section 501 refers only to customers, and does not instruct or authorize the Commission to establish safeguards covering other information.[35] However, other commenters who favored requiring safeguards for all nonpublic personal information noted flaws in this approach, namely, that: (1) Financial institutions may be unable to distinguish accurately between customer and consumer information,[36] and (2) consumers may not understand the customer-consumer distinction, and may believe that their information is subject to safeguards that do not apply to them.[37]

While the Commission believes that limiting the rule to ''customer information'' is warranted by the plain language of section 501,[38] it shares some of the concerns raised by the commenters who favored broader protections. In response, the Commission notes 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 the Privacy Rule and 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, proposed paragraphs (c) and (d) contain definitions of ''information security program'' and ''service provider.'' ''Information security program'' is defined 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 similar to the Banking Agency Guidelines' definition of ''customer information system.'' See Banking Agency Guidelines, section I.C.2.d. ''Service provider'' is defined as ''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 of ''service provider'' in the Banking Agency Guidelines. *See* Banking Agency Guidelines, section I.C.2.e. The Commission requests comment on both of these proposed definitions.

Proposed section 314.3: Standards for Safeguarding Customer Information

This section sets forth the general standards 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. *See* proposed paragraph (a). This standard is highly flexible, consistent with the comments and the Banking Agency Guidelines. It is also consistent with 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'' and that ''different types of data warrant different levels of protection.'' *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).

By requiring a written information security program, the Commission means to ensure a comprehensive, coordinated approach to security. As under the Banking Agency Guidelines, which also require a written program,[39] the program need not be set forth in a single document, as long as all parts of the program are coordinated and can be identified and accessed readily.[40] For this reason, and because of the general flexibility of the proposed rule's requirements, the Commission does not expect the preparation of a written program to be unduly burdensome. Nevertheless, the Commission requests comment on the benefits and burdens of this requirement and/or other issues or concerns that it raises; whether any burden is disproportionate for smaller entities; and how any burden can be lessened while still ensuring that each financial institution develops an effective program for which it is accountable.

Paragraph (b) of this section restates the objectives of section 501(b) of the Act and incorporates them as the objectives of the proposed rule.

Proposed Section 314.4: Elements

This section sets forth general elements that a financial institution should adopt as part of its information security program. The elements create a framework for developing, implementing, and maintaining the

[33] As noted above, the proposed rule would directly cover an affiliate that receives customer information from a financial institution and is itself a financial institution. Further, an affiliate that meets the definition of ''service provider'' in the proposed rule will be subject to contractural requirements to maintain safeguards. *See* proposed paragraph 314.5(d). Thus, other provisions of the proposed rule may already cover information handled or maintained by at least some affiliates.

[34] *See* Banking Agency Guidelines, section I.A.; see also ACA at 3–4; ACB at 3; Intuit at 3; MasterCard at 3; NCISS at 1; NRF at 2–3; NIADA at 1–2; TGSL at 2; Plainview at 1; Visa at 3; cf NAAG at 1–2 (supporting limitation, but urging that term ''customer information'' be broadly construed).

[35] *See, e.g.,* ACA at 3–4; TGSL at 2; Visa at 3.

[36] Ashley at 2; Intuit at 3; NAAG at 2; NACAA at 3.

[37] NACAA at 3.

[38] *See* section 501(a) & (b)(1)–(3). By contrast to section 501, the privacy provisions of the Act apply to both ''customers'' and ''consumers'' of financial institutions, but require greater disclosures to the former. *See* section 502(a) & (b) (consumers); section 503 (customers).

[39] *See* Banking Agency Guidelines, section II.A.

[40] *See* Preamble to the Banking Agency Guidelines, 66 FR 8619 (if the elements of the program ''are not maintained on a consolidated basis, management should have an ability to retrieve the current documents from those responsible for the overall coordination and ongoing reevaluation of the program.''

required safeguards, but leave each financial institution discretion to tailor its information security program to its own circumstances.[41]

Proposed paragraph (a) requires each financial institution to designate an employee or employees to coordinate its information security program in order to ensure accountability within each entity for achieving adequate safeguards. This requirement is similar to the Banking Agency Guidelines' requirements to involve and report to the Board of Directors. See Banking Agency Guidelines, Paragraphs III.A., and III.F., respectively. However, because many entities subject to the Commission's jurisdiction are not controlled by Boards of Directors, the rule permits a financial institution to designate any responsible employee or employees that it chooses. The Commission believes that this requirement will ensure accountability within a flexible framework.[42] The Commission seeks comment on the benefits and burdens of this paragraph and/or other issues or concerns that it raises, as well as whether there are effective alternative means to achieve accountability for compliance with the rule.

Proposed paragraph (b) requires 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.'' Because some of the comments sought further guidance on steps to take in conducting a risk assessment,[43] the proposed paragraph also requires financial institutions to consider such risks in each relevant area of their operations, including three areas of particular importance to information security: (1) Employee training and management; (2) information systems, including information processing, storage, transmission and disposal; and (3) prevention and response measures for attacks, intrusions, or other systems failures. This paragraph is similar to the Banking Agency Guidelines' requirement to assess risks,[44] but adds these core areas of operation in response to the comments. Beyond the three core areas of operation that a financial institution must consider, each entity would have discretion to determine what areas of its operation are relevant to risk assessment. The Commission seeks comment on the benefits and burdens of this paragraph and/or other issues or concerns that it raises; whether specifying certain areas of operation is helpful and appropriate; and/or whether additional guidance would be useful.[45]

Proposed paragraph (c) requires 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.'' As in paragraph (b), a financial institution must address each relevant area of its operations in developing its program.[46] The obligation to monitor (and, in paragraph (e), discussed below, to adjust in light of changes) the information security program is consistent with the Advisory Committee's findings that a security program should have ''a continuous life cycle'' and that companies should be prepared to ''revisit and revise [their security standards] on a constant basis.'' ACR at 18. It also is similar to the Banking Agency Guidelines' requirement to ''[r]egularly test the key controls, systems and procedures of the information security program.'' *See* Banking Agency Guidelines, paragraph III.C.3. Consistent with the commenters' support for the use of testing[47] but concern about the potential costs and effectiveness of such procedures,[48] the proposed rule does not require that particular audit procedures or tests be used. The Commission requests comment on the benefits and burdens of this paragraph and/or other issues or concerns that it raises.

Proposed paragraph (d) requires each financial institution to oversee its service providers. This obligation requires each financial institution to select and retain service providers ''that are capable of maintaining appropriate safeguards'' for the customer information at issue, and to require its service providers by contract to ''implement and maintain such safeguards.'' This provision, which is similar to a requirement in the Banking Agency Guidelines,[49] is intended to ensure that customer information will remain protected when it is shared with another entity to carry out processing, servicing, and similar functions on behalf of the financial institution. It also ensures that the obligation to safeguard information is not diminished simply because certain functions are outsourced rather than performed in-house. The Commission requests comment on the benefits and burdens of this requirement and/or other issues or concerns that it raises, including: (1) Whether additional guidance is needed on what safeguards are appropriate for service providers; (2) whether the contract requirement is necessary to ensure the protection of customer information or whether there is an equally protective alternative; (3) whether, for service providers that are themselves financial institutions or are subject to other safeguards standards, the rule should offer an exception to the contract requirement; and (4) whether the rule should apply to all service providers, given that the Privacy Rule does not require financial institutions to enter into confidentiality contracts with service providers that receive information under the general exceptions in sections 313.14 and 313.15 of that rule.

The Commission is aware that an entity providing services both to a financial institution subject to the Commission's rule and to one subject to the Banking Agency Guidelines could be subject to contractual obligations under both the proposed rule and the Guidelines, albeit for different sets of information. In some cases, a service

[41] Many of these procedures are similar to those identified by the Advisory Committee's Report as ''essential elements'' of an effective program. See ACR at 18 (assessment of risk, establishment and implementation of a plan based on the identified risks, and periodic reassessment of risks).

[42] This proposal responds to comments seeking flexibility in designating responsible employees. *See, e.g.,* Visa at 5 (suggesting the rule should allow financial institutions to designate either an individual, or a working group or committee); ACB at 4 (opposing idea of a single privacy officer); CUNA at 2 (same). *See also* NAAG at 2; MSDWCC at 3 (stating that designation of a privacy officer would ensure accountability).

[43] *See e.g.,* NIADA at; Intuit at 7–8.

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

[45] Consistent with the comments, the proposed rule does not require financial institutions to conduct risk assessment according to any predetermined schedule. See NIADA at 4; USA Funds at 3. However, as discussed below, proposed paragraph (e) requires that each financial institution adjust its program in light of any material changes to its business. The Commission envisions that the timeliness of such adjustments would be relevant to the adequacy of a financial institutions' safeguards under the rule.

[46] For example, in the area of employee training and management, an entity could implement a training program designed to combat the risk that unauthorized third parties could gain access to customer information. Or, with respect to its information systems, an entity could implement a particular protocol for disposing of customer information to control any risk that unauthorized parties could gain access to discarded information. Similarly, in the area of prevention and response measures for attacks and system failures, an entity could maintain appropriate controls or monitoring systems to deter and detect actual or attempted attacks or intrusions.

[47] *See, e.g.,* CUNA at 3; Intuit at 10; Tiger Testing 1–2.

[48] ACB at 5; USA Funds at 4.

[49] Banking Agency Guidelines, section III.D.

provider—such as a data processor—that is subject to such contractual obligations also would be a financial institution subject to the Commission's rule. The Commission believes, however, that the similarity of the proposed rule to the Banking Agency Guidelines, and the flexible standards of the proposed rule, should prevent any conflict. Nonetheless, comment is requested on any potential difficulty for service providers in complying simultaneously with these various requirements.

Proposed paragraph (e) requires 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. This paragraph is similar to section III.E. of the Banking Agency Guidelines. Such material changes may include, for example, changes in technology; changes to its operations or business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, or changes in the services provided; new or emerging internal or external threats to information security; or other circumstances that give it reason to know that its information security program is vulnerable to attack or compromise. The Commission seeks comment on the benefits and burdens of this requirement and/or other issues or concerns that it raises.

Proposed Section 314.5: Effective Date

Proposed section 314.5 requires each financial institution to implement an information security program not later than one year from the date on which a final rule is issued. The Commission requests comment on whether one year is an appropriate amount of time for covered entities to come into compliance with the rule. It also requests comment on whether the rule should contain a transition period to allow the continuation of existing contracts with service providers, even if they would not satisfy the rule's requirements. Such a provision could parallel section 313.18(c) of the Privacy Rule, which provides a two-year period for grandfathering existing contracts.

D. Paperwork Reduction Act

The Paperwork Reduction Act (''PRA''), 44 U.S.C. Chapter 35, requires federal agencies to seek and obtain Office of Management and Budget (''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'' when 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 Commission has determined that the proposed standards do not constitute a ''collection of information.'' The proposed rule calls upon affected entities to develop or strengthen their information security programs in order to provide reasonable safeguards. Each financial institution's means of complying with the rule will vary according to its size, complexity, the nature and scope of its activities, and the sensitivity of the information involved. Although these compliance efforts must be summarized in writing, the discretionary balancing of factors and circumstances that is involved here 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.

E. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA), 5 U.S.C. 604(a), requires an agency either to provide an Initial Regulatory Flexibility Analysis with a proposed rule, or certify that the proposed rule will not have a significant economic impact on a substantial number of small entities. The FTC does not expect that this rule, if adopted, would have the threshold impact on small entities. First, most of the burdens flow from the mandates of the Act, not from the specific provisions of the proposed rule. Second, the proposed rule imposes requirements that are scalable according to the size and complexity of each institution, the nature and scope of its activities, and the sensitivity of its information. Thus, the burden is likely to be less on small institutions, to the extent that their operations are smaller or less complex. Nonetheless, the Commission has determined that it is appropriate to publish an Initial Regulatory Flexibility Analysis (''IRFA'') in order to inquire into the impact of the proposed rule on small entities. The Commission invites comment on the burden on small entities that may result from this rulemaking, and has prepared the following analysis.

1. Reasons for the Proposed Rule

Section 501(b) of the G–L–B Act 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. The requirements of the proposed rule are intended to fulfill the obligations imposed by section 501(b).

2. Statement of Objectives and Legal Basis

The objectives of the proposed rule are discussed above. The legal basis for the proposed rule is section 501(b) of the G–L–B Act.

3. Description of Small Entities to Which the Rule Will Apply

Determining a precise estimate of the number of small entities that are financial institutions subject to the proposed rule is not readily feasible. 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. However, 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.

4. Projected Reporting, Recordkeeping and Other Compliance Requirements

The proposed rule does not impose any reporting or any specific recordkeeping requirements within the meaning of the PRA, discussed above. The proposed rule 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. In so doing, the institution must assure itself that any affiliate to which it discloses customer information maintains appropriate safeguards. In addition, each institution must designate an employee or employees to coordinate its safeguards; identify and assess foreseeable risks to customer information, and evaluate 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. These requirements will apply to institutions of all sizes that are subject to the FTC's jurisdiction.

A few comments received in response to the Notice expressed concern about the burden on small businesses of maintaining information security. The Commission has attempted to address these concerns by making the requirements flexible so that each entity can simplify its information security program to the same extent that its overall operations are simplified. Nonetheless, the Commission is concerned about the potential impact of the proposed rule on small institutions, and invites comment on the costs of establishing and operating an information security program for such entities, particularly any costs stemming from the proposed requirements to: (1) Designate an employee or employees to coordinate safeguards; (2) regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (3) develop a comprehensive information security program in written form; and (4) ensure that affiliates with which the entities share information maintain adequate safeguards.

5. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The FTC is unable to identify any statutes, rules, or policies that would conflict with the requirement to develop and implement an information security program. However, as discussed above, the Commission is requesting comment on the extent to which other federal standards involving privacy or security of information may duplicate and/or satisfy the proposed rule's requirements. In addition, the FTC seeks comment and information about any statutes or rules that may conflict with any of the proposed requirements, as well as any other state, local, or industry rules or policies that require a covered institution to implement business practices that comport with the requirements of the proposed rule.

6. Discussion of Significant Alternatives

The G–L–B Act requires the FTC to issue a rule that establishes standards for safeguarding customer information. In addition, the G–L–B Act requires that standards be developed for institutions of all sizes. Therefore, the proposed rule applies to entities with assets of $100 million or less. However, the standards in the proposed rule are flexible, so that each institution may develop an information security program that is appropriate to its size and the nature of its operations. The FTC welcomes comment on any significant alternatives, consistent with the G–L–B Act, that would minimize the impact on small entities.

Proposed Rule

List of Subjects for 16 CFR Part 314

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

For the reasons set forth in the preamble, the Federal Trade Commission proposes to amend 16 CFR Ch. I, Subchapter C, by adding a new part 314 to read as follows:

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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

§ 314.1 Purpose and scope.

(a) *Purpose.* This part (''rule''), 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 rule applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (''FTC'' or ''Commission'') has jurisdiction. This rule refers to such entities as ''you.'' The rule 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 rule or unless the context otherwise requires, the terms used in this rule 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, process, 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 the rule.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive written information security program that 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 rule, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this rule, 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 risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) employee training and management;

(2) information systems, including information processing, storage, transmission, and disposal; and

(3) prevention and response measures for attacks, intrusions, or other systems failures.

(c) For all relevant areas of your operations, including those set forth in paragraph (b) of this section, 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) selecting and retaining 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 any material changes to your business that may affect your safeguards.

§ 314.5 Effective date.

Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this rule not later than one year from the date on which a final rule is issued.

By direction of the Commission.

C. Landis Plummer,

Acting Secretary.

[FR Doc. 01–19338 Filed 8–6–01; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF THE TREASURY

Internal Revenue Service

26 CFR Parts 1 and 301

[REG–103735–00; REG–110311–98; REG–103736–00]

RIN 1545–AX81; 1545–AW26; 1545–AX79

Modification of Tax Shelter Rules II

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Cross-reference notice of proposed rulemaking.

SUMMARY: These proposed rules provide the public with additional guidance needed to comply with the disclosure rules under section 6011(a), the registration requirement under section 6111(d), and the list maintenance requirement under section 6112 applicable to tax shelters. The proposed rules affect corporations participating in certain reportable transactions, persons responsible for registering confidential corporate tax shelters, and organizers of potentially abusive tax shelters. In the rules and regulations portion of this issue of the **Federal Register**, the IRS is issuing temporary regulations modifying the rules relating to the requirement that certain corporate taxpayers file a statement with their Federal corporate income tax returns under section 6011(a) and the registration of confidential corporate tax shelters under section 6111(d). The text of those temporary regulations also serves as the text of these proposed regulations.

DATES: Written or electronic comments and requests for a public hearing must be received by October 31. 2001.

ADDRESSES: Send submissions to: CC:ITA:RU (REG–103735–00; REG–110311–98; REG–103736–00), room 5226, Internal Revenue Service, POB 7604, Ben Franklin Station, Washington, DC 20044. Submissions may be hand delivered between the hours of 8 a.m. and 5 p.m. to: CC:ITA:RU (REG–103735–00; REG–110311–98; REG–103736–00), Courier's Desk, Internal Revenue Service, 1111 Constitution Avenue NW., Washington DC. Alternatively, taxpayers may submit comments electronically via the Internet by selecting the ''Tax Regs'' option of the IRS Home Page or by submitting comments directly to the IRS Internet site at http://www.irs.gov/tax_regs/regslist.html.

FOR FURTHER INFORMATION CONTACT: Concerning the regulations, Danielle M. Grimm, (202) 622–3080; concerning submissions, Guy Traynor, (202) 622–7180 (not a toll-free number).

SUPPLEMENTARY INFORMATION:

Background

The temporary regulations amend the Income Tax Regulations (26 CFR part 1) regarding rules relating to the filing and records requirements for certain corporate taxpayers under section 6011. The temporary regulations also amend the temporary procedure and administration regulations (26 CFR part 301) regarding the registration of confidential corporate tax shelters under section 6111.

The text of the temporary regulations also serves as the text of these proposed regulations. The preamble to the temporary regulations explains the regulations.

Special Analyses

It has been determined that this notice of proposed rulemaking is not a significant regulatory action as defined in Executive Order 12866. Therefore, a regulatory assessment is not required. It has also been determined that section 553(b) of the Administrative Procedure Act (5 U.S.C. chapter 5) does not apply to these regulations. Because these regulations impose no new collection of information on small entities, a Regulatory Flexibility Analysis under the Regulatory Flexibility Act (5 U.S.C. chapter 6) is not required. Pursuant to section 7805(f) of the Internal Revenue Code, this notice of proposed rulemaking will be submitted to the Chief Counsel for Advocacy of the Small Business Administration for comment on its impact on small business.

Comments and Requests for a Public Hearing

Before these proposed regulations are adopted as final regulations, consideration will be given to any written comments (preferably a signed original and eight (8) copies) or electronically generated comments that are submitted timely to the IRS. The IRS and Treasury request comments on the clarity of the proposed rules and how they can be made easier to understand.

All comments will be available for public inspection and copying. A public hearing will be scheduled if requested in writing by any person that timely submits written comments. If a public hearing is scheduled, notice of the date, time, and place for the public hearing will be published in the **Federal Register**.

Drafting Information

The principal author of these regulations is Danielle M. Grimm, Office of the Associate Chief Counsel (Passthroughs and Special Industries).