FEDERAL TRADE COMMISSION

16 CFR Part 313

Privacy of Consumer Financial Information

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: In this document, the Federal Trade Commission (the ''Commission'' or ''FTC'') issues a Notice of Proposed Rulemaking that is required by Section 504(a) of the Gramm-Leach-Bliley Act, (the ''G-L-B Act'' or ''Act'') with respect to financial institutions and other persons under the Commission's jurisdiction, as set forth in Section 505(a)(7) of the Act. The Commission requests comment on this proposed privacy Rule. Section 504 of the Act requires the Commission and other federal agencies to issue regulations implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers to nonaffiliated third parties. Pursuant to Section 503 of the G-L-B Act, a financial institution must provide its customers with a notice of its privacy policies and practices. Section 502 of the Act prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution satisfies various disclosure requirements and the consumer has not elected to opt out of the disclosure. This proposed Rule would implement the requirements outlined above.

DATES: Comments must be received on or before March 31, 2000.

ADDRESSES: Written comments should be addressed to: Secretary, Federal Trade Commission, Room H–159, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. The Commission requests that commenters submit the original plus five copies, if feasible. Comments should also be submitted if possible, in electronic form, on either a 5¼ or a 3½ inch computer disk, with a disk label stating the name of the commenter and the name and version of the word processing program used to create the document. (Programs based on DOS or Windows are preferred. Files from other operating systems should be submitted in ASCII format.) Alternatively, the Commission will accept comments submitted to the following E-mail address: GLBRule@ftc.gov. Those commenters submitting comments by e-mail are advised to confirm receipt by consulting the postings on the Commission's website at *www.ftc.gov*. 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 Rule, 16 CFR Part 313—Comment.''

Comments related to the Paperwork Reduction Act should also be submitted to the Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503, Attention: Desk Officer for FTC.

FOR FURTHER INFORMATION CONTACT: Kellie A. Cosgrove or Clarke Brinckerhoff, Attorneys, Division of Financial Practices, Federal Trade Commission, Washington, DC 20580, 202–326–3224.

SUPPLEMENTARY INFORMATION:

Section A. Background

On November 12, 1999, President Clinton signed the G-L-B Act (Public Law 106–102, codified at 15 U.S.C. 6801 *et seq.*) into law. 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 to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. Title V also requires the Commission, along with the Federal banking agencies and other authorities (Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, Secretary of the Treasury, and Securities and Exchange Commission (hereinafter referred to collectively as ''the Agencies'')), after consulting with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, to prescribe such regulations as may be necessary to carry out the purposes of the provisions in Title V, Subtitle A, that govern disclosure of nonpublic personal information.

The Commission and the Agencies have prepared proposed rules to implement Subtitle A that are consistent and comparable to the extent possible, as is required by the statute. The Commission requests comment on all aspects of its proposed Rule, as well as comment on the specific provisions and issues highlighted in the Section-by-Section Analysis of the Proposed Rule, below.

Section B. Section-by-Section Analysis of the Proposed Rule

The discussion that follows explains in detail each section of the Commission's proposed Rule.

Section 313.1 Purpose and Scope

Proposed paragraph (a) of this section identifies three purposes of the Rule. First, the Rule requires a financial institution to provide notice in specified circumstances to consumers about the institution's privacy policies and practices. Second, the Rule describes the conditions under which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party. Third, the Rule provides a method for a consumer to ''opt out'' of the disclosure of that information to nonaffiliated third parties, subject to the exceptions in proposed §§ 313.9, 313.10, and 313.11, as discussed below.

Proposed paragraph (b) sets out the scope of the Commission's proposed Rule, and tracks the scope of enforcement set out in section 505(a)(7) of the G-L-B Act. This paragraph states that the Rule applies only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes. The principal type of entity subject to the Rule is a ''financial institution,'' a term which is very broad under the Act. Section 509(3) defines the term to mean ''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)). Those ''financial activities'' include not only a number of traditional financial activities specified in Section 4(k) itself,[1] but also those activities that the Federal Reserve Board has found to be closely related to banking,[2] or usual

[1] Section 4(k)(4)(A-E) states ''the following activities shall be considered to be financial in nature: (A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities. (B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State. (C) Providing financial, investment, or economic advisory services, including advising an investment company (as defined in section 3 of the Investment Company Act of 1940). (D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly. (E) Underwriting, dealing in, or making a market in securities.''

[2] Section 4(k)(4)(F). The Board's list of such activities is set forth in 12 CFR 225.28. They

in connection with the transaction of banking or other financial operations abroad.[3] The Commission invites comment on whether the activities as set forth in the Board regulations (many of which are listed in notes 2–3 below) may be interpreted narrowly under the language of those regulations.[4] Issues relating to the scope of the Act are also discussed in the Section-by-Section Analysis of the definition of the term ''financial institution'' in § 313.3(j).

Paragraph (b) lists some examples of ''financial institutions'' subject to Commission jurisdiction under the Act. The Commission is also authorized to enforce the Act against ''other persons'' who are not financial institutions, but receive protected information from a financial institution and are subject to the Act's restrictions on reuse of the information set forth in proposed § 313.12.

Section 313.2 Rule of Construction

Proposed § 313.2 of the Rule sets out a rule of construction intended to clarify the effect of the examples used in the Rule. Given the wide variety of transactions that Title V, Subtitle A, of the G-L-B Act covers, the Commission and Agencies propose to adopt rules of general applicability and provide examples of conduct that would, and would not, comply with the Rule. While the general rules are consistent among the Commission's and Agencies' proposals to the extent possible, the examples used by the Commission and individual agencies differ on occasion from those used by the other agencies in order to provide guidance that may be most meaningful to entities within a given agency's jurisdiction. These examples are not intended to be exhaustive; rather they are intended to provide guidance about how the Rule would apply in specific circumstances. The Commission invites comment on whether including examples in the Rule is useful and suggestions on additional or different examples that may be helpful in illustrating compliance with the Rule.

Section 313.3 Definitions

a. *Affiliate*. The proposed Rule adopts the definition of ''affiliate'' that is used in section 509(6) of the G-L-B Act. An affiliation will be found when one company ''controls'' (which is defined in § 313.3(g)), is controlled by, or is under common control with another company. The definition includes both financial institutions and entities that are not financial institutions.

b. *Clear and conspicuous*. Title V, Subtitle A, of the G-L-B Act and the proposed Rule require that various notices be ''clear and conspicuous.'' The proposed Rule defines this term to mean that the notice is reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice.

The proposed Rule does not mandate the use of any particular technique for making the notices clear and conspicuous, but instead allows each financial institution the flexibility to decide for itself how best to comply with this requirement. Ways in which a notice may satisfy the clear and conspicuous standard would include, for instance, using a plain-language caption, in a type set easily seen, that is designed to call attention to the information contained in the notice. Other plain language principles are provided in the examples that follow the general rule.

c. *Collect*. The proposed Rule defines ''collect'' to mean obtaining any information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information. Several sections of the proposed Rule (*see, e.g.*, §§ 313.6 and 313.7) impose obligations that arise when a financial institution collects information about a consumer. This proposed definition clarifies that these obligations arise when the information enables the user to identify a particular consumer. It also clarifies that the obligations arise regardless of whether a financial institution obtains the information from a consumer or from some other source.

d. *Company*. The proposed Rule defines ''company,'' which is used in the definition of ''affiliate,'' as any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

e. *Consumer*. The proposed Rule defines ''consumer'' to mean an individual who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes. An individual also will be deemed to be a consumer of a financial institution if that institution purchases the individual's account from some other institution. The definition also includes the legal representative of an individual.

The G-L-B Act distinguishes ''consumers'' from ''customers'' for purposes of the notice requirements imposed by the Act. As explained more fully in the discussion of proposed § 313.4, below, a financial institution is required to give a ''consumer'' the notices required under Title V, Subtitle A, only if the institution intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party for a purpose that is not authorized by one of several exceptions set out in proposed §§ 313.10 and 313.11. By contrast, a financial institution must give all ''customers'' a notice of the institution's privacy policy at the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship.

A person is a ''consumer'' under the proposed Rule if he or she obtains a financial product or service from a financial institution. The definition of ''financial product or service'' in proposed § 313.3(k), below, includes,

include in certain circumstances: brokering or servicing loans; leasing real or personal property (or acting as agent, broker, or advisor in such leasing) without operating, maintaining or repairing the property; appraising real or personal property; check guaranty, collection agency, credit bureau, and real estate settlement services; providing financial or investment advisory activities including tax planning, tax preparation, and instruction on individual financial management; management consulting and counseling activities (including providing financial career counseling); courier services for banking instruments; printing and selling checks and related documents; community development or advisory activities; selling money orders, savings bonds, or traveler's checks; and providing financial data processing and transmission services, facilities (including hardware, software, documentation or operating personnel), data bases, advice, or access to these by technological means.

[3] Section 4(k)(4)(G). The scope of the Act is not limited to activities abroad, because the text of Section 4(k)(4)(G) is ''Engaging, in the United States, in any activity that (i) a bank holding company may engage in outside of the United States; and (ii) the Board has determined [by regulation in effect on November 11, 1999] to be usual in connection with the transaction of banking and financial operations abroad.'' (Emphasis added.) The Board has provided a list of such activities in 12 CFR 211.5(d). They include leasing real or personal property (or acting as agent, broker, or advisor in such leasing) where the lease is functionally equivalent to an extension of credit; acting as fiduciary; providing investment, financial, or economic advisory services; and operating a travel agency in connection with financial services.

[4] For example, 12 CFR 225.28(b)(1) and (b)(2) includes ''Extending credit and servicing loans'' and ''Activities related to extending credit'' as activities that are closely related to banking. Subsection (b)(2) delineates activities related to extending credit: real estate and personal property appraising; check guaranty services; collection agency services; credit bureau services; and real estate settlement servicing. The Commission requests comment on whether an entity engaged in (for example) real estate settlement servicing is a ''financial institution'' only if it also extends credit or services loans, or whether real estate settlement servicing alone constitutes a financial activity that results in an entity that engages in that activity being classified as a ''financial institution.'' Similarly, 12 CFR 211.5(d)(15) includes operating a travel agency ''in connection with financial services * * *'' The Commission requests comment on how the quoted language limits the activity of operating a travel agency, and the extent to which travel agencies are in fact operated in connection with financial services.

among other things, the evaluation by a financial institution of an application that a person submits to obtain a financial product or service. Thus, a financial institution that intends to share nonpublic personal information about a consumer with nonaffiliated third parties, outside of the exceptions described in §§ 313.10 and 313.11, will have to give the requisite notices, even if the consumer does not enter into a customer relationship with the institution.

The examples that follow the definition of ''consumer'' clarify when someone is a consumer. They include situations where someone applies for credit or provides information for the purpose of determining whether he or she prequalifies for a loan, or a person provides information in connection with seeking to obtain financial advisory services. The examples also clarify the status of someone whose credit account has been sold.

f. *Consumer reporting agency*. The proposed Rule adopts the definition of ''consumer reporting agency'' that is used in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)). This term is used in proposed §§ 313.11 and 313.13.

g. *Control*. The proposed Rule defines ''control'' using the tests applied in section 23A of the Federal Reserve Act (12 U.S.C. 371c). This definition is used to determine when companies are affiliated (*see* discussion of proposed § 313.3(a) above), and would result in financial institutions being considered affiliates regardless of whether the control is by a company or individual. The Commission invites comment on whether ''control'' should be defined by a more flexible standard than the percentage test set forth in proposed § 313.3(g)(1).

h. *Customer*. The proposed Rule defines ''customer'' as any consumer who has a ''customer relationship'' with a particular financial institution. As is explained more fully in the discussion of proposed § 313.4 below, a consumer becomes a customer of a financial institution at the time of entering into a continuing relationship with the institution. Thus, for instance, a consumer would become a customer at the time the consumer executes the documents needed to borrow money from a financial institution, or agrees to employ a broker to obtain (or try to obtain) a mortgage loan.

The distinction between consumers and customers determines what notices a financial institution must provide. If a consumer never becomes a customer, the institution is not required to provide any notices to the consumer unless the institution intends to disclose nonpublic personal information about that consumer to nonaffiliated third parties outside of the exceptions as set out in proposed §§ 313.10 and 313.11. By contrast, if a consumer becomes a customer, the institution must provide a copy of its privacy policy prior to the time it establishes the customer relationship and at least annually thereafter during the continuation of the customer relationship even if the institution is not going to share the consumer's information with nonaffiliated third parties.

i. *Customer relationship*. The proposed Rule defines ''customer relationship'' as a continuing relationship between a consumer and a financial institution whereby the institution provides a financial product or service to a consumer that is to be used primarily for personal, family, or household purposes. The Commission has interpreted the Act as requiring more than isolated transactions between a financial institution and a consumer to establish a customer relationship. The proposed Rule defines ''customer relationship'' as being of a ''continuing'' nature in order to encompass those business dealings that are not isolated, including those that involve a consumer becoming a client of the institution. As noted in the examples that follow the definition, these would include, for instance, cases where an institution opens a credit account for the consumer, a loan broker undertakes to assist a consumer to obtain a home mortgage, or an automobile dealer helps a consumer arrange credit to purchase a vehicle.

A one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. The examples that follow the definition of ''customer relationship'' clarify, for instance, that the purchase of an insurance policy would be sufficient to establish a customer relationship, whereas using an automated teller machine at a bank at which a consumer transacts no other business, cashing a check, purchasing travelers checks or money orders, or making a wire transfer would not. Similarly, simply purchasing airline tickets would not establish a customer relationship.[5] While a person engaging in one of these latter types of transactions would be a consumer under the regulation (thereby requiring the financial institution to provide notices *if* the institution intends to disclose nonpublic personal information about the consumer to nonaffiliated third parties outside of the exceptions), the consumer would not be a customer. A consumer would not necessarily become a customer simply by repeatedly engaging in isolated transactions, such as withdrawing funds at regular intervals from an ATM owned by an institution with whom the consumer has no account.

The examples also clarify that a consumer will have a customer relationship with a financial institution that makes a loan to the consumer and then sells the loan but retains the servicing rights. In that case, the person will be a customer of both the institution that sold the loan and the institution that bought it.

A consumer has a ''customer relationship'' with a debt collector that purchases an account from the original creditor (because he or she would have a credit account with the collector), but not with a debt collector that simply attempts to collect amounts owed to the creditor. However, the latter type of debt collector would still be generally bound by the limits on redisclosure and reuse of nonpublic personal information as set forth in proposed § 313.12.[6]

j. *Financial institution*. The proposed Rule adopts the definition of ''financial institution'' that is used in the G-L-B Act, namely, 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)). The exceptions to this definition contained in the G-L-B Act also are set out in the proposed Rule. As indicated by proposed §§ 313.3(j)(2) and 313.3(j)(3)(iv), the Commission views an entity as a financial institution ''the business of which is engaging in financial activities'' only if it is significantly engaged in a financial activity. Thus, a retail business that issues its own credit card directly to consumers is a financial institution engaged in the extension of credit, but a retail business that merely establishes

[5] Thus, an institution that operated a travel agency in connection with financial services would have a customer relationship with an individual for whom it plans a trip, but not with an individual to whom it simply sells tickets or traveler's checks (even on a repeated basis). The Commission specifically requests information on (1) the extent to which travel agencies are operated in connection with financial services and (2) the nature of specific business relationships that exist between consumers and such travel agents, as well as more general comments on the application of the proposed Rule to travel agents.

[6] This includes data obtained by the collector in collecting the debt because proposed § 313.3(o)(2)(E) specifically includes information obtained by a creditor's ''agent in connection with collecting on a loan'' in the definition of ''personally identifiable financial information.'' The Commission specifically requests comment on the application of the proposed Rule to debt collectors.

layaway or deferred payment plans is not a financial institution. The Commission invites comment concerning whether ''significantly engaged'' should be specifically defined in the Rule and, if so, how such a definition should be drafted. The Commission also invites comment on whether an individual who otherwise meets the definition (for example the sole proprietor of a mortgage loan brokerage business) can be a financial institution.

Due to the wide range of activities that are defined as financial in nature under Section 4(k) of the Bank Holding Company Act, the definition of ''financial institution'' encompasses a broad spectrum of businesses. (*See* discussion of the scope of the Act and the Rule at § 313.1.) The Commission recognizes that the plain meaning of the Act mandates this broad scope and requests general comment on this interpretation as well as comment on the application of the Rule to what might be considered the nontraditional financial institutions included in its scope.[7]

Many entities that come within the broad definition of financial institution will likely not be subject to the disclosure requirements of the Rule because not all financial institutions have ''consumers'' or establish ''customer relationships.'' For example, management consulting is a ''financial activity'' but it is not likely that any individual obtains management consulting services for personal, family or household purposes. Likewise, courier services and data processors who perform services for a financial institution, but do not provide financial products or services to individuals, will not be required to make the disclosures mandated by the Rule because they do not have ''consumers'' or ''customers'' as defined by the Rule.[8] The Commission invites comment on these and other entities that may be ''financial institutions'' under the Act, but may not be subject to the disclosure requirements of the Rule because they have no ''consumers'' or ''customers'' under the Rule.

Proposed § 313.3(j)(3)(iii) also incorporates the Act's exception for institutions chartered by Congress to engage in secondary market sales and similar transactions related to consumers, as long as the institution does not sell or transfer nonpublic personal information to a third party. The Commission interprets this exception in its proposed Rule to apply even if the chartered institution sells or transfers information as permitted by the exceptions to the notice and opt out requirements in proposed §§ 313.10 and 313.11. The proposed Rule reflects this interpretation. The Commission invites comment on this interpretation and on whether those entities that receive consumers' nonpublic personal information from such chartered institutions are nonetheless subject to the Rule's limitations on reuse. The Commission also seeks comment on whether chartered institutions should be required to enter into a confidentiality agreement with those nonaffiliated third parties with whom they share information pursuant to §§ 313.10 and 313.11 as a condition of their exemption.

k. *Financial product or service.* The proposed Rule defines ''financial product or service'' as a product or service that a financial holding company could offer by engaging in an activity that is financial in nature under section 4(k) of the Bank Holding Company Act of 1956. It includes the financial institution's evaluation of information collected in connection with an application by a consumer for a financial product or service. The proposed Rule states that the definition includes the financial institution's evaluation of information collected in connection with an application by a consumer for a financial product or service even if the application ultimately is rejected or withdrawn. It also includes the distribution of information about a consumer for the purpose of assisting the consumer in obtaining a financial product or service (by, for example, a mortgage broker or automobile dealer).

A product or service that does not result from a financial activity is not within the definition, even if the business is a financial institution; thus, a department store that issues its own credit card directly to consumers provides a financial service (credit) to consumers who utilize the card, but when it sells merchandise, it provides a nonfinancial product or service (retail sale of merchandise).

l. *Government regulator.* The proposed Rule adopts the definition of ''government regulator'' that includes the Commission, the Agencies, and state insurance authorities under the circumstances identified in the definition. This term is used in the exception set out in proposed § 313.11(a)(4) for disclosures to law enforcement agencies, ''including government regulators.''

m. *Nonaffiliated third party.* The proposed Rule defines ''nonaffiliated third party'' as any person (which includes natural persons as well as business entities such as corporations, partnerships, trusts, and so on) except (1) an affiliate of a financial institution, and (2) a joint employee of a financial institution and a third party. This definition is intended to be substantively the same as the definition used in Section 509(5) of the G-L-B Act.

n. *Nonpublic personal information.* Section 509(4) of the G-L-B Act defines ''nonpublic personal information'' to mean ''personally identifiable financial information'' (which term is not defined in the Act) that is provided by a consumer to a financial institution, results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. The definition of ''nonpublic personal information'' also includes any list, description, or other grouping of consumers—and ''publicly available information'' (which also is undefined in the G-L-B Act) pertaining to them—that is derived using any nonpublic personal information other than publicly available information.''

The proposed Rule implements this provision of the G-L-B Act by restating, in paragraph (1) of proposed § 313.3(n), the categories of information described above. However, the proposed Rule presents two alternatives (labeled Alternative A and Alternative B) concerning the treatment, for purposes of the definition of ''nonpublic personal information,'' of information that can be obtained from sources available to the general public.

The alternatives are based on differences in the definitions of ''personally identifiable financial information'' and ''publicly available information,'' which, when read together, result in more information being treated as ''nonpublic personal information'' under Alternative A than would be the case under Alternative B. The primary difference arises in the two definitions of ''publicly available information.'' Under Alternative A, information is ''publicly available information'' only if the financial

[7] These may include, but are not limited to: personal property appraisers; real estate appraisers; career counselors for employees in financial occupations; digital signature services; courier services; real estate settlement services; manufacturers of computer software and hardware; and travel agencies operated in connection with financial services.

[8] If such financial institutions receive consumers' nonpublic personal information from nonaffiliated financial institutions pursuant to one of the exceptions set forth in §§ 313.10 and 313.11, they would be required to observe the § 313.12 limitations on reuse of that information.

institution actually obtains the information from a public source. Under Alternative B, information is ''publicly available information'' if it could be obtained from a public source, regardless of its actual source. The Commission invites comment on both Alternatives. The Commission also invites comment on whether a variation of Alternative A and Alternative B should be adopted that would require a financial institution to undertake reasonable procedures to establish that information is, in fact, available from public sources before the financial institution may disclose it without restriction as ''publicly available information.''

The two Alternatives are substantially similar when viewed in the context of a list, but differ considerably in what information a financial institution can disclose about an individual who is not included on a list. Based on the definitions of ''publicly available information'' and ''personally identifiable financial information'' under Alternative A, any information that a financial institution obtains from an individual consumer is ''nonpublic personal information'' and cannot be disclosed by the financial institution without first providing notice and opt out to the consumer. Under Alternative B, however, if that same information could be obtained from public sources, the definitions dictate that the information is not ''nonpublic personal information'' and the financial institution may disclose it without restriction as ''publicly available information.'' Thus, if a consumer provided name and address as part of an application for a financial product or service, a financial institution could not, under Alternative A, disclose the consumer's name and address without providing notice and opt out. Under Alternative B, however, if that same individual consumer's name and address could otherwise be obtained from a public source, the financial institution could disclose it without restriction.

While an *individual* consumer's information may be treated differently under the two Alternatives, a *list* of consumers receives virtually identical protection. Both alternatives include in the definition of ''nonpublic personal information'' any list, description, or other grouping of consumers that is derived using ''personally identifiable financial information.'' The proposed Rule makes clear that ''personally identifiable financial information'' includes the fact that an individual is a consumer or customer of a financial institution. Therefore, any list of a financial institution's customers is nonpublic personal information because it is necessarily derived from the fact of the customer relationship.[9] Thus, under Alternative B, even if the names and addresses of the financial institution's customers could have been obtained from a public source (and are, therefore, publicly available), the financial institution cannot reveal them as part of a customer list because that list was derived using personally identifiable financial information (the fact of the customer relationship).[10]

o. *Personally identifiable financial information.* As discussed above, the G-L-B Act defines ''nonpublic personal information'' to include, among other things, ''personally identifiable financial information'' but does not define the latter term.

As a general matter, the proposed Rule treats any personally identifiable information as financial if it is obtained by a financial institution in connection with providing a financial product or service to a consumer. The Commission believes that this approach reasonably interprets the word ''financial'' and creates a workable and clear standard for distinguishing information that is financial from other personal information. The Commission recognizes that this interpretation may result in certain information being covered by the rules that may not be considered intrinsically financial, such as health status, and specifically invites comment on the proposed definition of ''personally identifiable financial information.''

The proposed Rule defines ''personally identifiable financial information'' to include three categories of information. While the three categories are for the most part identical in both Alternatives (*see* discussion concerning differences in the third category, below), the differences in how Alternatives A and B treat publicly available information result in different applications of what ''personally identifiable financial information'' is included within the definition of ''nonpublic personal information.''

The first category of information considered to be ''personally identifiable financial information'' is any information that a consumer provides to a financial institution in order to obtain a financial product or service. As noted in the examples that follow the definition, this would include information provided on an application to obtain a loan, credit card, or other financial product or service. If, for instance, medical information is provided on an application to obtain a financial product or service (such as would be the case if a consumer applies for a life insurance policy), that information would be considered ''personally identifiable financial information'' for purposes of the proposed Rule.

The second category of information covered by the proposed definition of ''personally identifiable financial information'' includes any information resulting from any transaction between the consumer and the financial institution involving a financial product or service. This would include, as noted in the examples following the definition, account balance information, payment or overdraft history, and credit or debit card purchase information.

The third category includes any financial information about a consumer otherwise obtained by the financial institution in connection with providing a financial product or service. This would include, for example, information obtained from a consumer report or from an outside source to verify information a consumer provides on an application to obtain a financial product or service. There is a difference in the statement of this third category between Alternatives A and B. Alternative A expressly excludes from this category ''publicly available information,'' while Alternative B does not. However, given the definitions of ''nonpublic personal information'' and ''publicly available information'' in Alternative B, the result is that any of the three categories of personally identifiable financial information in Alternative B will exclude publicly available information from the personally identifiable financial information that is considered ''nonpublic personal information.''

The examples clarify that the definition of ''personally identifiable information'' does not include a list of names and addresses of people who are customers of an entity that is not a financial institution. Thus, the names and addresses of people who subscribe, for instance, to a particular magazine fall outside the definition. If, however, a financial institution discloses those

[9] If the fact of the customer relationship could be obtained from the public record, under Alternative B the list is not derived from ''personally identifiable financial information'' and the notice and opt out requirements are not implicated (as long as the names and addresses could be obtained from the public record). Thus, under Alternative B, a list of a financial institution's mortgage customers is not ''nonpublic personal information'' if all of the information on the list could be obtained from public sources.

[10] Under Alternative A, the names and addresses themselves are ''personally identifiable financial information'' if the financial institution did not actually obtain them from the public record.

names and addresses as part of a list of the institution's customers, then the names and addresses become nonpublic personal information.

The Commission notes that there are other laws that may impose limitations on disclosures of nonpublic personal information in addition to those imposed by the G-L-B Act and this proposed Rule. For instance, the Fair Credit Reporting Act imposes conditions on the sharing of application information and credit report information between affiliates and nonaffiliated third parties.[11] The recently proposed Department of Health and Human Services regulations[12] that implement the Health Insurance Portability and Accountability Act of 1996 would, if adopted in final, limit the circumstances under which medical information may be disclosed. There may be State laws that affect a financial institution's ability to disclose information. Thus, financial institutions will need to comply with relevant laws and monitor legislative and regulatory developments that affect the disclosure of consumer information.

The Commission seeks comment on whether further definition of ''personally identifiable'' would be helpful.

p. *Publicly available information.* The proposed Rule contains two versions of the definition of ''publicly available information.'' The definitions differ in that Alternative A does not treat information as publicly available unless it is obtained from one of the public sources listed in the proposed Rule. Alternative B, by contrast, treats information as publicly available if it could be obtained from one of the public sources listed in the rules, even if it was obtained from a source not listed in the definition. The Commission invites comment on which alternative is more appropriate.

The remaining parts of the two alternative versions are identical. Thus, under either alternative, the definition of ''publicly available information'' includes information from official public records, such as real estate recordations or security interest filings. It also includes information from widely distributed media (such as a telephone book, television or radio program, or newspaper) and information that is required to be disclosed to the general public by Federal, State, or local law (such as securities disclosure documents). The proposed Rule states that information obtained over the Internet will be considered publicly available information if the information is obtainable from a site available to the general public without requiring a password or similar restriction. The Commission invites comment on what information is appropriately considered publicly available, particularly in the context of information available over the Internet.

(q) *You* includes each ''financial institution'' (but excludes any ''other person'') over which the Commission has enforcement jurisdiction pursuant to Section 505(a)(7) of the Act.

§ 313.4 Initial Notice to Customers and Consumers of Privacy Policies and Practices Required.

Initial notice required. The G-L-B Act requires a financial institution to provide an initial notice of its privacy policies and practices in two circumstances. For customers, the notice must be provided at the time of establishing a customer relationship. For consumers who do not become customers, the notice must be provided prior to disclosing nonpublic personal information about the consumer to a nonaffiliated third party. In addition, as discussed more fully in § 313.8(c) below, a revised notice must be provided to such consumers prior to disclosing nonpublic personal information to nonaffiliated third parties if a financial institution's policies or practices have changed and previous notices do not accurately describe the financial institution's policies or practices.

Paragraph (a) of proposed § 313.4 states the general rule regarding these notices. Pursuant to that paragraph, a financial institution must provide a clear and conspicuous notice (*i.e.,* a notice that is reasonably understandable and designed to call attention to the nature and significance of the information it provides) that accurately reflects the institution's privacy policies and practices. Thus, a financial institution may not fail to maintain the protections that it represents in the notice that it will provide. The Commission expects that financial institutions will take appropriate measures to adhere to their stated privacy policies.

The proposed Rule does not prohibit affiliated institutions from using a common initial, annual, or opt out notice, so long as the notice is delivered in accordance with the Rule and is accurate for all recipients. Similarly, the Rule does not prohibit an institution from establishing different privacy policies and practices for different categories of consumers, customers, or products, so long as each customer or consumer receive a notice that is accurate with respect to him or her.

Notice to customers. The proposed Rule requires that a financial institution provide a privacy notice to the consumer prior to the time that it has established a customer relationship. Thus, the notices may be provided at the same time a financial institution is required to give other notices, such as those required by the Board's regulations implementing the Truth-in-Lending Act. (12 CFR § 226.6) This approach is intended to strike a balance between (1) ensuring that consumers will receive privacy notices at a meaningful point along the continuum of ''establishing a customer relationship'' and (2) minimizing unnecessary burdens on financial institutions that may result if a financial institution is required to provide a consumer with a series of notices at different times in a transaction. Nothing in the proposed Rule is intended to discourage a financial institution from providing an individual with a privacy notice at an earlier point in the relationship if the institution wishes to do so in order to make it easier for the consumer to compare its privacy policies and practices with those of other financial institutions in advance of conducting transactions.

Paragraph (c) of proposed § 313.4 identifies the time a customer relationship is established as the point at which a financial institution and a consumer enter into a continuing relationship. The examples that are provided after the statement of the general rule inform the reader that, for customer relationships that are contractual in nature (including, for example, loans), a customer relationship is established upon the execution by the consumer of the contract that is necessary to conduct the transaction in question. In the case of a credit card account, the customer relationship is established when the consumer opens the account. A consumer opens a credit card account when he or she becomes obligated on the account, such as when he or she makes the first purchase, receives the first advance, or becomes

[11] The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 *et seq,* provides no limitation at all on communication by an entity of its own ''transactions or experiences'' with the consumer (*e.g.,* the individual's account history). However, it strictly limits the reporting of information obtained from other sources, such as consumer applications or credit reports. An institution may normally share such data with its affiliates only if it has complied with the notice and opt-out procedures set forth in FCRA § 603(d)(2)(A)(iii), which are very similar to those set forth in Section 502(b)(1) of the Act. Sharing such data with nonaffiliates may be effectively prohibited in most cases by the FCRA, because the institution would become a consumer reporting agency subject to its restrictions on reporting of information to third parties.

[12] 64 FR 59918 (Nov. 3, 1999).

obligated for any fee or charge under the account other than an application fee or refundable membership fee. For transactions that may not involve a contract (including, for instance, providing investment advisory, loan brokerage, or tax preparation services), a customer relationship will be established when the consumer pays or agrees to pay a fee or commission for the service, and/or becomes a client of the business.

Notice to consumers. For consumers who do not establish a customer relationship, the initial notice may be provided at any point before the financial institution discloses nonpublic personal information to nonaffiliated third parties. An initial notice is not required, as provided in paragraph (b) of the proposed Rule, if the institution does not intend to disclose the information in question or intends to make only those disclosures that are authorized by one of the exceptions set out in §§ 313.10 and 313.11 of the proposed Rule.

How to provide notice. Paragraph (d) of proposed § 313.4 sets out the rules governing how financial institutions must provide the initial notices. The general rule requires that the initial notice be provided so that each recipient can reasonably be expected to receive actual notice. The Commission invites comment on whether, when there is more than one party to an account, there are instances where all parties to the account need not receive the notice.

The notice may be delivered in writing or, if the consumer agrees, electronically. Oral notices alone are insufficient. In the case of customers, the notice must be given in a way so that the customer may either retain it or access it at a later time. This requirement that the notice be given in a manner permitting access at a later time does not preclude a financial institution from changing its privacy policy. *See* proposed § 313.8(c), below. Rather, the Rule is intended only to require that a customer be able to access the most recently adopted privacy policy.

Examples of acceptable ways the notice may be delivered include hand-delivering a copy of the notice, mailing a copy to the consumer's last known address, or sending it via electronic mail to a consumer who obtains a financial product or service from the institution electronically. It would not be sufficient to provide only a posted copy of the notice in a lobby. Similarly, it would not be sufficient to provide the initial notice only on a Web page, unless the consumer is required to access that page to obtain the product or service in question. Electronic delivery generally should be in the form of electronic mail so as to ensure that a consumer actually receives the notice. In those circumstances where a consumer is in the process of conducting a transaction over the Internet, electronic delivery also may include posting on a Web page as described above. If a financial institution and consumer orally agree to enter into a contract for a financial product or service over the telephone, the institution may provide the consumer with the option of receiving the initial notice after providing the product or service so as not to delay the transaction. The Commission invites comment on the regulatory burden of providing the initial notices and on the methods financial institutions anticipate using to provide the notices.

The Commission recognizes that in some circumstances a customer does not have a choice as to the institution with which he or she has a customer relationship, such as when an institution purchases the customer's loan in the secondary market. In these situations, it may not be practicable for the institution to provide a notice prior to the time the customer relationship is established. The proposed Rule provides that if a financial institution purchases a loan or assumes a deposit liability from another financial institution or in the secondary market and the customer does not have a choice about the purchase or assumption, the acquiring financial institution may provide the initial notice within a reasonable time thereafter. The Commission invites comment on whether there are other similar situations for which an exception is necessary.

The Commission also recognizes that certain consumers may have requested that a financial institution not send statements, notices, or other communications to them, such as in certain private banking relationships. The Commission requests comment on whether and how the Rule should address these situations with respect to the notices required by this Rule. The Commission also requests comment on whether there are other situations where providing notice by mail is impracticable.

Section 313.5 Annual Notice to Customers of Privacy Policies and Practices Required

Section 503 of the G-L-B Act requires a financial institution to provide notices of its privacy policies and practices at least annually to its customers. The proposed Rule implements this requirement by requiring a clear and conspicuous notice that accurately reflects the privacy policies and practices then in effect to be provided at least once during any period of twelve consecutive months. The rules governing how to provide an initial notice also apply to annual notices.

Section 503(a) of the G-L-B Act requires that the annual notices be provided ''during the continuation'' of a customer relationship. To implement this requirement, the proposed Rule states that a financial institution is not required to provide annual notices to a customer with whom it no longer has a continuing relationship. The examples that follow this general rule provide guidance on when there no longer is a continuing relationship for purposes of the Rule. These include, for instance, loans that are paid in full or charged off, or accounts sold without retaining servicing rights.

There will be certain customer relationships (such as obtaining investment advice from a stock broker) that do not present a clear event after which there is no longer a customer relationship. The proposed Rule contains an example intended to cover these situations, stating that a relationship will no longer be deemed continuing for purposes of the proposed Rule if the financial institution has not communicated with a customer, other than providing an annual privacy policy notice, for a period of 12 consecutive months.

The Commission invites comment generally on whether the examples provided in proposed § 313.5 are adequate and on whether the proposed standard deeming an account relationship to have terminated after 12 months of no communication is appropriate. The Commission also invites comment on the regulatory burden of providing the annual notices and on the methods financial institutions anticipate using to provide the notices.

Section 313.6 Information to be Included in Initial and Annual Notices of Privacy Policies and Practices

Section 503 of the G-L-B Act identifies the items of information that must be included in a financial institution's initial and annual notices. Section 503(a) of the G-L-B Act sets out the general requirement that a financial institution must provide customers with a notice describing the institution's policies and practices with respect to, among other things, disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) of the Act identifies

certain elements that must be addressed in that notice.

The required content is the same for both the initial and annual notices of privacy policies and practices. While the information contained in the notices must be accurate as of the time the notices are provided, a financial institution may prepare its notices based on current and anticipated policies and practices.

The information to be included is as follows:

1. *Categories of nonpublic personal information that a financial institution may collect.* Section 503(b) requires a financial institution to inform its customers about the categories of nonpublic personal information that the institution collects. The proposed Rule implements this requirement in proposed § 313.6(a)(1) and provides an example of how to comply with this requirement that focuses the notice on the source of the information collected. As noted in the example, a financial institution will satisfy this requirement if it categorizes the information according to the sources, such as application information, transaction information, and credit report information. Financial institutions may provide more detail about the categories of information collected but are not required to do so by the proposed Rule.

2. *Categories of nonpublic personal information that a financial institution may disclose.* Section 503(a)(1) of the G-L-B Act requires the financial institution's initial and annual notice to provide information about the categories of nonpublic personal information that may be disclosed either to affiliates or nonaffiliated third parties.

The proposed Rule implements this requirement in proposed § 313.6(a)(2). The examples of how to comply with this rule focus on the content of the information to be disclosed. As stated in the relevant examples, a financial institution may satisfy this requirement by categorizing information according to source and providing illustrative examples of the content of the information. These categories might include application information (such as assets and income), identifying information (such as name, address, and social security number), transaction information (such as information about account activity, account balances, and purchases), and information from credit reports (such as credit history).

Financial institutions are free to provide more detailed information in the initial and annual notices if they choose to do so. Conversely, if a financial institution does not disclose, and does not intend to disclose, nonpublic personal information to affiliates or nonaffiliated third parties, its initial and annual notices may simply state this fact without further elaboration about categories of information disclosed.

3. *Categories of affiliates and nonaffiliated third parties to whom a financial institution discloses nonpublic personal information.* As previously noted, section 503(a) includes a general requirement that a financial institution provide a notice to its customers of the institution's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) states that the notice required by section 503(a) shall include certain specified items. Among those is the requirement, set out in section 503(b)(1), that a financial institution inform its consumers about its policies and practices with respect to disclosing nonpublic personal information to nonaffiliated third parties. The Commission believes that, when read together, Sections 503(a) and 503(b) of the G-L-B Act require a financial institution's notice to address disclosures of nonpublic personal information to both affiliates and nonaffiliated third parties.

The proposed Rule implements this requirement in § 313.6(a)(3). The example illustrating how a financial institution may comply with the Rule states that a financial institution will adequately categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic personal information about consumers if it identifies the types of businesses in which they engage. Types of businesses may be described by general terms only if the financial institution provides illustrative examples of the significant lines of businesses of the recipient. The Commission's intent is that any illustrations must be reasonably designed to be meaningful to consumers. Proposed § 313.6 includes examples of general types of businesses and appropriate corresponding illustrative examples for each. Other appropriate examples include an institution that referred to ''retail stores'' and explained that this includes grocery stores and drug stores, or to ''manufacturers of consumer products'' and provided meaningful examples such as pharmaceutical products and children's toys.

The G-L-B Act does not require a financial institution to list the categories of persons to whom information may be disclosed pursuant to one of the exceptions set out in proposed §§ 313.10 and 313.11. The proposed Rule states that a financial institution is required only to inform customers that it makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the notice. The Commission invites comment on whether such a notice would be adequate.

If a financial institution does not disclose, and does not intend to disclose, nonpublic personal information to affiliates or nonaffiliated third parties, its initial and annual notices may simply state this fact without further elaboration about categories of third parties.

4. *Information about former customers.* Section 503(a)(2) of the Act requires the financial institution's initial and annual privacy notices to include the institution's policies and practices with respect to disclosing the nonpublic personal information of persons who have ceased to be customers of the institution. Section 503(b)(1)(B) requires that this information be provided with respect to information disclosed to nonaffiliated third parties.

The Commission has concluded that, when read together, Sections 503(a)(2) and 503(b)(1)(B) require a financial institution to include in the initial and annual notices the institution's policies and practices with respect to sharing information about former customers with all affiliates and nonaffiliated third parties. This requirement is set out in the proposed Rule at § 313.6(a)(4). This requirement does not require a financial institution to provide a notice and opportunity to opt out to a former customer before sharing nonpublic personal information about that former customer with an affiliate.

5. *Information disclosed to service providers.* Section 502(b)(2) of the G-L-B Act permits a financial institution to disclose nonpublic personal information about a consumer to a nonaffiliated third party for the purpose of the third party performing services for the institution, including marketing financial products or services under a joint agreement between the financial institution and at least one other financial institution. In this case, a consumer has no right to opt out. However, the financial institution must inform the consumer that it will be disclosing the information in question, unless the service falls within one of the exceptions listed in Section 502(e) of the Act.

Proposed § 313.6(a)(5) implements these provisions by requiring that, if a financial institution discloses nonpublic personal information to a nonaffiliated third party pursuant to the exception for service providers and joint marketing,

the institution is to include in the initial and annual notices a separate description of the categories of information that are disclosed and the categories of third parties providing the services. However, proposed §§ 313.6(a)(3) and (a)(4) specify that no disclosure is required if a financial institution discloses nonpublic personal information to a nonaffiliated third party service provider pursuant to proposed §§ 313.10 or 313.11. A financial institution may comply with these requirements by providing the same level of detail in the notice as is required to satisfy the requirements in proposed §§ 313.6(a)(2) and (3).

6. *Right to opt out.* As previously noted, Sections 503(a)(1) and 503(b)(1) of the G-L-B Act require a financial institution to provide customers with a notice of its privacy policies and practices concerning, among other things, disclosing nonpublic personal information consistent with Section 502 of the Act.

Proposed § 313.6(a)(6) implements this requirement by requiring the initial and annual notices to explain the right to opt out of disclosures of nonpublic personal information to nonaffiliated third parties, including the methods available to exercise that right.

7. *Disclosures made under the FCRA.* Section 503(b)(4) of the G-L-B Act requires a financial institution's initial and annual notice to include the disclosures required, if any, under Section 603(d)(2)(A)(iii) of the FCRA. Section 603(d)(2)(A)(iii) excludes from the definition of ''consumer report'' the communication of certain consumer information among affiliated entities if the consumer is notified about the disclosure of such information and given an opportunity to opt out of that information sharing. The information that can be shared among affiliates under this provision includes, for instance, information from consumer reports and applications for financial products or services. In general, this information represents personal information provided directly by the consumer to the institution, such as income and social security number, in addition to information contained within credit bureau reports.

The proposed Rule implements Section 503(b)(4) of the G-L-B Act by including the requirement that a financial institution's initial and annual notice include any disclosures a financial institution is required to make under Section 603(d)(2)(A)(iii) of the FCRA.

8. *Confidentiality, security, and integrity.* Section 503(a)(3) of the G-L-B Act requires the initial and annual notices to provide information about a financial institution's policies and practices with respect to protecting the nonpublic personal information of consumers. Section 503(b)(3) of the Act requires the notices to include the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information, in accordance with section 501 (which requires the Commission and the Agencies to establish standards governing the administrative, technical, and physical safeguards of customer information).

The proposed Rule implements these provisions by requiring a financial institution to include in the initial and annual notices the institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information. The relevant example in the proposed Rule states that a financial institution may comply with the requirement as it concerns confidentiality and security if the institution explains matters such as who has access to the information and the circumstances under which the information may be accessed. The information about integrity should focus on the measures the institution takes to protect against reasonably anticipated threats or hazards. The proposed Rule does not require a financial institution to provide technical or proprietary information about how it safeguards consumer information.

The Commission is in the process of preparing the section 501 standards, and will publish a separate notice of proposed rulemaking concerning them as soon as practicable.

§ 313.7 Limitation on Disclosure of Nonpublic Personal Information About Consumers to Nonaffiliated Third Parties

Section 502(a) of the G-L-B Act generally prohibits a financial institution from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution provides the consumer with a notice of the institution's privacy policies and practices. Section 502(b) further requires that the financial institution provide the consumer with a clear and conspicuous notice that the consumer's nonpublic personal information may be disclosed to nonaffiliated third parties, that the consumer be given an opportunity to opt out of that disclosure, and that the consumer be informed of how to opt out.

Section 313.7 of the proposed Rule implements these provisions. Paragraph (a)(1) of § 313.7 sets out the criteria that a financial institution must satisfy before disclosing nonpublic personal information to nonaffiliated third parties. As stated in the text of the proposed Rule, these criteria apply to direct and indirect disclosures through an affiliate. The Commission invites comment on how the right to opt out should apply in the case of joint accounts. Should, for instance, a financial institution require all parties to an account to opt out before the opt out becomes effective? If not, and only one of the parties opts out, should the opt out apply only to information about the party opting out or should it apply to all parties to the account?

Paragraph (a)(2) defines ''opt out'' in a way that incorporates the exceptions to the right to opt out stated in proposed §§ 313.9, 313.10, and 313.11.

The proposed Rule implements the requirement that a consumer be given an opportunity to opt out before information is disclosed by requiring that the opportunity be reasonable. The examples that follow the general rule provide guidance in situations involving notices that are mailed and notices that are provided in connection with isolated transactions. In the former case, a consumer will have a reasonable opportunity to opt out if the financial institution provides 30 days in which to opt out. In the latter case, an opportunity will be reasonable if the consumer must decide as part of the transaction whether to opt out before completing the transaction. The Commission invites comment on whether 30 days is a reasonable opportunity to opt out in the case of notices sent by mail, and on whether an example in the context of transactions conducted using an electronic medium would be helpful.

The requirement that a consumer have a reasonable opportunity to opt out does not mean that a consumer forfeits that right once the opportunity lapses. The consumer always has the right to opt out (as discussed further in proposed § 313.8, below). However, if an individual does not exercise that opt out right when first presented with an opportunity, the financial institution would be permitted to disclose nonpublic personal information to nonaffiliated third parties for some period of time necessary to implement the consumer's opt out direction.

Paragraph (b) of proposed § 313.7 clarifies that the right to opt out applies regardless of whether a consumer has established a customer relationship with a financial institution. As noted above, all customers are consumers under the proposed Rule. Thus, the fact that a

consumer establishes a customer relationship with a financial institution does not change the institution's obligations to comply with the requirements of proposed § 313.7(a) before sharing nonpublic personal information about that consumer with nonaffiliated third parties. This also applies in the context of a consumer who had a customer relationship with a financial institution but then terminated that relationship. Paragraph (b) also clarifies that the consumer protections afforded by paragraph (a) of proposed § 313.7 apply to all nonpublic personal information collected by a financial institution, regardless of when collected. Thus, if a consumer elects to opt out of information sharing with nonaffiliated third parties, that election applies to all nonpublic personal information about that consumer in the financial institution's possession, regardless of when the information is obtained.

Paragraph (c) of proposed § 313.7 states that a financial institution may, but is not required to, provide consumers with the option of a partial opt out in addition to the opt out required by this section. This could enable a consumer to limit, for instance, the types of information disclosed to nonaffiliated third parties or the types of recipients of the nonpublic personal information about that consumer. If the partial opt out option is provided, a financial institution must state this option in a way that clearly informs the consumer about the choices available and consequences thereof.

Section 313.8 Form and Method of Providing Opt Out Notice to Consumer

Paragraph (a) of proposed § 313.8 requires that any opt out notice provided by a financial institution pursuant to proposed § 313.7 be clear and conspicuous and accurately explain the right to opt out. The notice must inform the consumer that the institution may disclose nonpublic personal information to nonaffiliated third parties, state that the consumer has a right to opt out, and provide the consumer with a reasonable means by which to opt out.

The examples that follow the general rule state that a financial institution will adequately provide notice of the right to opt out if it identifies the categories of information that may be disclosed and the categories of nonaffiliated third parties to whom the information may be disclosed and that the consumer may opt out of those disclosures. A financial institution that plans to disclose only limited types of information, or to only a specific type of nonaffiliated third party, may provide a correspondingly narrow notice to consumers. However, to minimize the number of opt out notices a financial institution must provide, the institution may wish to base its notices on current and anticipated information sharing plans. A new opt out notice is required if the financial institution discloses information to different types of nonaffiliated third parties, or discloses different types of information, unless the most recent opt out notice is sufficiently broad to cover the entities or information in question. Nor is a financial institution required to provide a subsequent opt-out notice when a consumer establishes a new type of customer relationship with that financial institution, unless the institution's opt out policies differ depending on the type of customer relationship.

The examples also suggest several ways in which a financial institution may provide reasonable means to opt out, including check-off boxes, reply forms, self-addressed stamped envelopes, toll-free phone numbers, and electronic mail addresses. A financial institution does not provide a reasonable means to opt out if the only means provided is for a consumer to write his or her own letter to the institution to exercise the right, although an institution may honor such a letter if received. The Commission invites comment on whether financial institutions should be required to accept opt outs through any means the institution has already established to communicate with consumers. For example, if a financial institution has established a toll free telephone number for its customer service department, should the institution be required to accept opt outs at that number? Similarly, if a financial institution has established a Web site, should it be required to accept opt outs at that site?

Paragraph (b) applies the same rules to delivery of the opt out notice that apply to delivery of the initial and annual notices. In addition, paragraph (b) clarifies that the opt out notice may be provided together with, or on the same form as, the initial and annual notices. However, if the opt out notice is provided after the initial notice, a financial institution must provide a copy of the initial notice along with the opt out notice. If a financial institution and consumer orally agree to enter into a customer relationship, the institution may provide the opt out notice within a reasonable time thereafter if the consumer agrees. The Commission invites comment on whether a more specific time by which the notice must be given would be appropriate.

Paragraph (c) sets out the rules governing a financial institution's obligations in the event the institution changes its disclosure policies. As stated in that paragraph, a financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless the institution first provides a revised notice and new opportunity to opt out. The institution must wait a reasonable period of time before disclosing information according to the terms of the revised notice in order to afford the consumer a reasonable opportunity to opt out. A financial institution must provide the revised notice of its policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under §§ 313.4(c) and 313.8(b), respectively, which require that the notices be given in a manner so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form.

Paragraph (d) states that a consumer has the right to opt out at any time. The Commission considered whether to include a time limit by which financial institutions must effectuate a consumer's opt out election, but decided that the wide variety of practices of financial institutions made one limit inappropriate. Instead, the Commission's proposed Rule requires that the disclosures stop as soon as reasonably practicable. The Commission solicits comment on whether it would be more appropriate to require a specific time to implement these opt-outs.

Paragraph (e) states that an opt out will continue until a consumer revokes it. The proposed Rule requires that such revocation be in writing, or, if the consumer has agreed, electronically.

The Commission invites comment on the likely burden of complying with the requirement to provide opt out notices, the methods financial institutions anticipate using to deliver the opt out notices, and the approximate number of opt out notices they expect to deliver and process.

Section 313.9 Exception to opt out Requirements for Service Providers and Joint Marketing

Section 502(b) of the G–L–B Act creates an exception to the opt-out rules for the disclosure of information to a nonaffiliated third party for use by the third party to perform services for, or functions on behalf of, the financial institution, including the marketing of the financial institution's own products

or services or financial products or services offered pursuant to a joint agreement between two or more financial institutions.[13] A consumer will not have the right to opt out of disclosing nonpublic personal information about the consumer to nonaffiliated third parties under these circumstances, if the financial institution satisfies certain requirements.

First, the institution must, as stated in section 502(b), ''fully disclose'' to the consumer that it will provide this information to the nonaffiliated third party before the information is shared. This disclosure should be provided as part of the initial notice that is required by § 313.4. The Commission invites comment on whether the proposed Rule appropriately implements the ''fully disclose'' requirement in section 502(b)(2).

Second, the financial institution must enter into a contract with the third party that requires the third party to maintain the confidentiality of the information. This contract should be designed to ensure that the third party (a) will maintain the confidentiality of the information at least to the same extent as is required for the financial institution that discloses it, and (b) will use the information solely for the purposes for which the information is disclosed or as otherwise permitted by §§ 313.10 and 313.11 of the proposed Rule. The Commission invites comment on whether third party contractors should be permitted to use information received pursuant to proposed § 313.9 to improve credit scoring models or analyze marketing trends, as long as the third parties do not maintain the information in a way that would permit identification of a particular consumer.

Section 502(b)(2) of the G–L–B Act allows the Commission to impose requirements on the disclosure of information pursuant to the exception for service providers beyond those imposed in the statute. The Commission has not done so in the proposed Rule, but invites comment on whether additional requirements should be imposed, and, if so, what those requirements should address. The Commission also invites comments on any other requirements that would be appropriate to protect a consumer's financial privacy, and on whether the Rule should provide examples of the types of joint agreements that are covered.

Section 313.10 Exceptions for Processing and Servicing Transactions

Section 502(e) of the G–L–B Act creates exceptions to the requirements that apply to the disclosure of nonpublic personal information to nonaffiliated third parties. Paragraph (1) of that section sets out certain exceptions for disclosures made, generally speaking, in connection with the administration, processing, servicing, and sale of a consumer's account.

Paragraph (a) of proposed § 313.10 sets out those exceptions, making only stylistic changes to the statutory text that are intended to make the exceptions easier to read. Paragraph (b) sets out the definition of ''necessary to effect, administer, or enforce'' that is contained in section 509(7) of the G–L–B Act, making only stylistic changes intended to clarify the definition.

The exceptions set out in proposed § 313.10, and the exceptions discussed in proposed § 313.11, below, do not affect a financial institution's obligation to provide initial notices of its privacy policies and practices prior to the time it establishes a customer relationship and annual notices thereafter. Those notices must be provided to all customers, regardless of whether the institution intends to disclose the nonpublic personal information.

Section 313.11 Other Exceptions to opt out Requirements

As noted above, section 502(e) contains several exceptions to the requirements that otherwise would apply to the disclosures of nonpublic personal information to nonaffiliated third parties. Proposed § 313.11 sets out those exceptions that are not made in connection with the administration, processing, servicing, and sale of a consumer's account, and makes stylistic changes intended to clarify the exceptions.

One of the exceptions stated in proposed § 313.11 is for disclosures made with the consent or at the direction of the consumer, provided the consumer has not revoked the consent. Following the list of exceptions is an example of consent in which a financial institution that has received an application from a consumer for a mortgage loan informs a nonaffiliated insurance company that the consumer has applied for a loan so that the insurance company can contact the person about homeowner's insurance. Consent in such a situation would enable the financial institution to make the disclosure to the third party without first providing the initial notice required by § 313.4 or the opt out notice required by § 313.7, but the disclosure must not exceed the purposes for which consent was given. The example also states that consent may be revoked by a consumer at any time by the consumer exercising the right to opt out of future disclosures. The Commission intends that a ''consent'' that was not clearly made by a consumer (for example, one in the form of a line buried in a document or a negative option not clearly explained to the consumer) would not provide an effective exception to the opt-out right. The Commission invites comment on whether specific safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion. Such safeguards might include, for instance, a requirement that consent be written or that it be indicated on a separate signature line in a relevant document or on a distinct Web page, or that it may be effective for only a limited period of time.

Section 313.12 Limits on Redisclosure and Reuse of Information

Section 313.12 of the proposed Rule implements the Act's limitations on redisclosure and reuse of nonpublic personal information about consumers. Section 502(c) of the Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not, directly or indirectly through an affiliate, disclose the information to any person that is not affiliated with either the financial institution or the third party, unless the disclosure would be lawful if made directly by the financial institution. Paragraph (a)(1) sets out the Act's redisclosure limitation as it applies to a financial institution that receives information from another nonaffiliated financial institution. Paragraph (b)(1) mirrors the provisions of paragraph (a)(1), but applies the redisclosure limits to any nonaffiliated third party that receives nonpublic personal information from a financial institution.

The Act appears to place the institution that receives the information into the shoes of the institution that disclosed the information for purposes of determining whether redisclosures by the receiving institution are ''lawful.'' Thus, the Act appears to permit the receiving institution to redisclose the information only to: (1) An entity to whom the original transferring institution could disclose the information pursuant to one of the exceptions in § 313.9, 313.10, or 313.11;

[13] Section 502(e) also sets forth some exceptions for transmitting information to third parties for servicing and processing purposes, and exempts them from the notice, as well as the opt-out, provisions of the Act. These are discussed in more detail in §§ 313.10 and 313.11. In those cases, the consumer has no disclosure or opt-out rights.

or (2) an entity to whom the original transferring institution could have disclosed the information as described under its notice of privacy policies and practices, unless the consumer has exercised the right to opt out of that disclosure. Because a consumer can exercise the right to opt out of a disclosure at any time, the Act may effectively preclude third parties that receive information to which the opt out right applies from redisclosing the information, except pursuant to one of the exceptions in §§ 313.9, 313.10, or 313.11. The Commission invites comment on whether the Rule should require a financial institution that discloses nonpublic personal information to a nonaffiliated third party to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of that information.

Sections 502(b)(2) and 502(e) (as implemented by §§ 313.9, 313.10, and 313.11 of the proposed Rule) describe when a financial institution may disclose nonpublic personal information without providing the consumer with initial privacy notice and an opportunity to opt out, but those exceptions apply only when the information is used for the specific purposes set out in those sections. Paragraph (a)(2) of proposed § 313.12 clarifies this limitation on reuse as it applies to financial institutions. Paragraph (a)(2) provides that a financial institution may use nonpublic personal information about a consumer that it receives from a nonaffiliated financial institution in accordance with an exception under §§ 313.9, 313.10, or 313.11 only for the purpose of that exception. Paragraph (b)(2) applies the same limits on reuse to any nonaffiliated third party that receives nonpublic personal information from a financial institution. The Commission requests comment on whether proposed §§ 313.12(a)(2) and 313.12(b)(2) would restrict a nonaffiliated third party from using information obtained in accordance with the exceptions in §§ 313.9, 313.10, and 313.11 for purposes beyond the scope of those exceptions if the information is not used in a personally identifiable form. This might occur, for example, in the case of a credit scoring vendor using information to improve its scoring models.

The Commission invites comments on the meaning of the word ''lawful'' as that term is used in section 502(c). The Commission specifically solicits comment on whether it would be lawful for a nonaffiliated third party to disclose information pursuant to the exception provided in proposed § 313.9 of the Rule. Under that exception, a financial institution must comply with certain requirements before disclosing information to a nonaffiliated third party. Given that the statute and proposed Rule impose those requirements on the financial institution making the initial disclosure, the Commission invites comment on whether subsequent disclosures by the third party could satisfy the requirement that those disclosures be lawful when the financial institution is not party to the subsequent disclosure.

Section 313.13 Limits on Sharing of Account Number Information for Marketing Purposes

Section 502(d) of the G–L–B Act prohibits a financial institution from disclosing, other than to a consumer reporting agency, account numbers or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. Proposed § 313.13 applies this statutory prohibition to disclosures made directly or indirectly by a financial institution.

The Commission notes that there is no exception in Title V, Subtitle A, to the flat prohibition established by section 502(d). The Statement of Managers contained in the Conference Report to S. 900 encourages the Commission and Agencies to adopt an exception to section 502(d) to permit disclosures of account numbers in limited instances. It states:

> In exercising their authority under section 504(b) [which vests the Commission and Agencies with authority to grant exceptions to section 502(a)–(d) beyond those set out in the statute], the agencies and authorities described in section 504(a)(1) may consider it consistent with the purposes of this subtitle to permit the disclosure of customer account numbers or similar forms of access numbers or access codes in an encrypted, scrambled, or similarly coded form, where the disclosure is expressly authorized by the customer and is necessary to service or process a transaction expressly requested or authorized by the customer.

Managers' Statement at 18. The Commission has not proposed an exception to the prohibition of section 502(d) because of the risks associated with third parties' direct access to a consumer's account. The Commission seeks comment on whether an exception to the section 502(d) prohibition that permits third parties access to account numbers is appropriate, the circumstances under which an exception would be appropriate, and how such an exception should be formulated to provide consumers with adequate protection. The Commission also seeks comment on whether a flat prohibition as set out in section 502(d) might unintentionally disrupt certain routine practices, such as the disclosure of account numbers to a service provider who handles the preparation and distribution of monthly account statements for a financial institution coupled with a request by the institution that the service provider include marketing literature with the statement about a product. In addition, the Commission invites comment on whether a consumer ought to be able to consent to the disclosure of his or her account number, notwithstanding the general prohibition in section 502(d) and, if so, what standards should apply. The Commission also seeks comment on whether section 502(d) prohibits the disclosure by a financial institution to a marketing firm of encrypted account numbers if the financial institution does not provide the marketer the key to decrypt the number.

Section 313.14 Protection of Fair Credit Reporting Act

Section 506 makes several amendments to the FCRA to vest rulemaking authority in various agencies and to restore the Agencies' regular examination authority. Paragraph (c) of section 506 states that, except for the amendments noted regarding rulemaking authority, nothing in Title V, Subtitle A is to be construed to modify, limit, or supersede the operation of the FCRA, and no inference is to be drawn on the basis of the provisions of Title V, Subtitle A as to whether information is transaction or experience information under section 603 of the FCRA.

Proposed § 313.14 implements section 506(c) of the G–L–B Act by restating the statute, making only minor stylistic changes intended to make the Rule clearer.

Section 313.15 Relation to State Laws

Section 507 of the G–L–B Act states, in essence, that Subtitle A of Title V does not preempt any state law that provides greater protections than are provided by that Subtitle of the Act. Determinations of whether a State law or Subtitle A of Title V provides greater protections are to be made by the Commission after consultation with the agency that regulates either the party filing a complaint or the financial institution about whom the complaint was filed. Determinations of whether

State or Federal law afford greater protections may be initiated by any interested party or on the Commission's own motion.

Proposed § 313.15 is substantively identical to section 507, noting that the proposed Rule (as opposed to the statute) does not preempt state laws that provide greater protection for consumers than does the Rule.

Section 313.16 Effective Date; Transition Rule

Section 510 of the G–L–B Act states that, as a general rule, the relevant provisions of Subtitle A of Title V take effect 6 months after the date on which rules are required to be prescribed. However, section 510(1) authorizes the Commission and the Agencies to prescribe a later date in the rules enacted pursuant to section 504.

Proposed § 313.16 states, in paragraph (a), an effective date of November 13, 2000. This assumes that a final Rule will be enacted within the time frame prescribed by section 504(a)(3). The Commission intends to provide at least six months following the adoption of a final Rule for financial institutions to bring their policies and procedures into compliance with the requirements of the final Rule. The Commission invites comment on whether six months following adoption of a final Rule is sufficient to enable financial institutions to comply with the Rule.

Paragraph (b) of proposed § 313.16 provides a transition rule for consumers who were customers as of the effective date of the Rule. Since those customer relationships already will have been established as of the Rule's effective date (thereby making it inappropriate to require a financial institution to provide those customers with a copy of the institution's initial notice at the time of establishing a customer relationship), the Rule requires instead that the initial notice be provided within 30 days of the effective date. The Commission invites comment on whether 30 days is enough time to permit a financial institution to deliver the required notices, bearing in mind that the G–L–B Act contemplates at least a six-month delayed effective date from the date the Rule is adopted.

If a financial institution intends to disclose nonpublic personal information about someone who was a consumer before the effective date, the institution must provide the notices required by §§ 313.4 and 313.7 and provide a reasonable opportunity to opt out before the effective date. If, in this instance, the institution already is disclosing information about such a consumer, it may continue to do so without interruption until the consumer opts out, in which case the institution must stop disclosing nonpublic personal information about that consumer to nonaffiliated third parties as soon as reasonably practicable.

Section C. Invitation to Comment

Before adopting this Rule as final, the Commission will give consideration to any written comments submitted to the Secretary of the Commission on or before March 31, 2000. Comments submitted will be available for public inspection in accordance with the Freedom of Information Act (5 U.S.C. 552) and Commission regulations, on normal business days between the hours of 8:30 a.m. and 5 p.m. at the Public Reference Section, Room 130, Federal Trade Commission, 600 Pennsylvania Avenue NW., Washington, DC 20580. Comments will also be posted on the Commission website; <*www.ftc.gov*>.

Section D. Communications by Outside Parties to Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding from any outside party to any Commissioner or Commissioner's advisor will be placed on the public record. *See* 16 CFR. § 1.26(b)(5) (1998).

Section E. Regulatory Flexibility Act

The Commission believes that the proposed Rule's requirements are expressly mandated by the G–L–B Act, and the Act's requirements account for most, if not all, of the economic impact of the proposed Rule. While the Commission believes that it could certify that the proposed Rule will not have a significant impact on a substantial number of small entities, the Commission has decided, nonetheless, to publish the following initial regulatory flexibility analysis pursuant to the Regulatory Flexibility Act, 5 U.S.C. 601–612, as amended, and request public comment on the impact on small businesses of its proposed Rule implementing the G–L–B Act.

Description of the Reasons That Action by the Agency is Being Considered

Section 504 of the G–L–B Act requires the Commission to promulgate this Rule not later than six months after the date of enactment of the Act, or May 12, 2000.

Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

To implement the disclosure requirements and restrictions on certain financial institutions' abilities to disclose nonpublic personal information about consumers to nonaffiliated third parties. The legal basis for the proposed Rule is Section 504 of the G–L–B Act.

Description of and, Where Feasible, an Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

In general, the Rule will apply to any financial institution subject to the Commission's jurisdiction that shares nonpublic personal information with nonaffiliated third parties or that establishes customer relationships with consumers. The definition of ''financial institution'' includes any institution the business of which is engaging in a financial activity, as defined under 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). (G–L–B Act § 509(3)(A).) A precise estimate of the number of small entities that are financial institutions within the meaning of the proposed Rule is not currently feasible. In addition, of those small entities that are financial institutions, there is no way to precisely estimate the number that share consumers' nonpublic personal information with nonaffiliated third parties or that establish customer relationships with consumers. The Commission seeks any information or comment on these issues, as noted below.

Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Proposed 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

The statute and proposed Rule do not directly impose any ''reporting'' or ''recordkeeping'' requirements on financial institutions within the meaning of the Paperwork Reduction Act, but would require that financial institutions, in specified circumstances, make certain third party disclosures to the public. These disclosures include: notice of the financial institution's privacy policy to consumers at the time of establishing a customer relationship with a consumer (Proposed Rule § 313.4); annual notice of the financial institution's privacy policy to those consumers with whom it continues to have a customer relationship (Proposed Rule § 313.5); notice to consumers, regardless of whether a customer relationship has been established, of a financial institution's privacy policy and notice and opportunity to opt-out

prior to the financial institution's sharing of a consumer's nonpublic personal information with nonaffiliated third parties (Proposed Rule § 313.8(a)); and notice to customers of any changes that the financial institution makes in its policies concerning sharing nonpublic personal information with nonaffiliated third parties (Proposed Rule § 313.8(c)). The Commission is seeking clearance from the Office of Management and Budget (''OMB'') for these requirements and the Commission's Supporting Statement submitted as part of that process will be made available on the public record of this rulemaking.

Because the proposed Rule does not directly mandate ''reporting'' or ''recordkeeping'' within the meaning of the Paperwork Reduction Act, the Rule does not require professional skills for the preparation of ''reports'' or ''records'' under the Act. The disclosures and other burdens referenced above likely will require some amount of managerial and/or professional (including attorney), clerical, and in some instances, skilled technical time to develop and disseminate the required disclosures. For purposes of its Supporting Statement to OMB under the Paperwork Reduction Act, the Commission estimated that the average yearly burden over the three-year period of clearance is 4.03 million hours and $87.3 million. The Commission, as noted below, seeks further comment on the costs and burdens of small entities in complying with the requirements of the proposed Rule.

Identification, to the Extent Practicable, of all Relevant Federal Rules That May Duplicate, Overlap or Conflict With the Proposed Rule

While the scope of the proposed Rule is unique, there may be some overlap in certain circumstances with other Federal laws. Because there is a relationship between the proposed requirements and the notice requirements under the Fair Credit Reporting Act (''FCRA''), 15 U.S.C. 1681–1681u, the proposed Rule requires that the financial institution's initial and annual notices shall also include any disclosure that it is required to make under the FCRA. (Rule § 313.6(a)(7).) Also, at the time a consumer contracts for an electronic fund transfer service, the Electronic Funds Transfer Act requires the terms and conditions of such transfer to be disclosed, including under what circumstances the entity will in the ordinary course of business disclose information concerning the consumer's account to third persons. Finally, the Children's Online Privacy Protection Act generally requires online service operators collecting personal information from a child to obtain parental consent and post a privacy notice on the Website. As noted below, the Commission seeks comment and information on any other rules that may be duplicative, overlapping, or in conflict with this proposed rule.

Description of any significant alternatives to the proposed Rule that accomplish the stated objectives of applicable statutes and that minimize any significant economic impact of the proposed Rule on small entities, including alternatives considered, such as: (1) Establishment of differing compliance or reporting requirements or timetables that take into account resources available to small entities; (2) clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) use of performance rather than design standards; (4) any exemption from coverage of the rule, or any part thereof, for such small entities. In drafting the proposed Rule, the Commission has made every effort to avoid unduly burdensome requirements for financial institutions of all sizes. In a number of respects the proposed Rule is flexible and allows financial institutions to select methods of compliance that are reasonable, taking into account the financial institution's business practices and capabilities.

For example, financial institutions that are required to provide disclosures to consumers must provide the notice so that the consumer can reasonably be expected to actually receive it. (Proposed Rule § 313.4(d).) The proposed Rule allows the financial institutions to choose a delivery method that imposes the least burden on the financial institution while also complying with the statutory mandate that the consumer be provided with the appropriate disclosures. Regarding the law's clear and conspicuous requirements, the proposed Rule does not mandate the use of any particular technique for making the notices clear and conspicuous, but instead allows each financial institution the flexibility to decide for itself how best to comply with this requirement. (Proposed Rule § 313.4(b).) In addition, the proposed Rule requires that a financial institution provide the opportunity to opt-out directly to a consumer but provides alternate means of providing that notice—a small entity, or any entity, can choose a means that is reasonable taking into account its circumstances. (Proposed Rule § 313.8(b).) No recordkeeping requirement has been included in the proposed Rule. Thus, no entity, regardless of size, is unnecessarily burdened by recordkeeping requirements.

The Commission has made every effort to minimize the burden on small entities—and all entities—and to be reasonable in its rulemaking. To that end, the Commission has clarified the breadth of the statutory term ''financial institution'' to include an institution significantly engaged in a financial activity. (Proposed Rule § 313.3(j).) The effect of this definition is twofold: it encompasses and subjects to its requirements those institutions that are not solely in the business of a financial activity but that are significantly engaged in such an activity as part of their business; and excludes from coverage those entities, large or small, that may engage in financial activities as some small, insignificant portion of their business.

The proposed Rule also provides for a streamlined version of the content of an institution's privacy policy for any entity that does not share nonpublic personal information with third parties. (Proposed Rule § 313.4(b).) Thus, entities of any size that do not share information are not unduly burdened. Moreover, those financial institutions, regardless of size, that engage in only one-time isolated transactions with consumers are not required to provide a privacy policy to consumers unless they intend to share the consumer's nonpublic personal information with a nonaffiliated third party. (Proposed Rule § 313.4(b).)

Questions for Comment To Assist Regulatory Flexibility Analysis

1. Please provide information or comment on the number and type of small entities affected by the proposed Rule. Include in your comments the number of small entities that share consumers' nonpublic personal information with nonaffiliated third parties or that establish customer relationships with consumers.

2. Please provide comment on any or all of the provisions in the proposed Rule with regard to (a) the impact of the provision(s) (including any benefits and costs), if any, the Commission should consider, as well as the costs and benefits of those alternatives, paying specific attention to the effect of the Rule on small entities in light of the above analysis. Costs to implement and comply with the Rule include expenditures of time and money for: any employee training; attorney or other

professional time; preparing relevant materials; and processing materials.

3. Please describe ways in which the Rule could be modified to reduce any costs or burdens for small entities consistent with the G–L–B Act's mandated requirements.

4. Please provide any information quantifying the economic benefits to financial institutions of sharing consumers' nonpublic personal information.

5. Please identify all relevant Federal, state or local rules that may duplicate, overlap or conflict with the proposed Rule. In addition, please identify any industry rules or policies that require financial institutions to implement business practices (*e.g.*, disclosure of privacy policy and right to opt-out, etc.) that would already comply with the requirements of the Commission's proposed Rule.

Section F. Paperwork Reduction Act

The Commission has submitted this proposed Rule to the Office of Management and Budget for review under the Paperwork Reduction Act (''PRA'') (44 U.S.C. 3501–3517). As required by the G–L–B Act, the proposed Rule specifies disclosure requirements for financial institutions subject to the Commission's jurisdiction that are subject to the requirements of PRA. The required disclosures include: (1) Initial notice of the financial institution's privacy policy at the time it establishes a customer relationship with a consumer and/or prior to its sharing a consumer's nonpublic personal information with nonaffiliated third parties; (2) notice of the consumer's right to opt-out of information sharing with nonaffiliated third parties; (3) annual notice of the financial institution's privacy policy to any continuing customer; and (4) notice to consumers when the financial institution changes its practices on information sharing with nonaffiliated third parties. Although the proposed Rule's disclosure requirements are expressly required by the G–L–B Act, the Commission has adopted a performance standard to provide flexibility in implementing the requirements.

The Commission has estimated the paperwork burden of the proposed Rule for financial institutions that are subject to the Commission's jurisdiction, based on staff's knowledge of the financial services industry. Under Section 505(a)(7) of the G–L–B Act, the Commission has jurisdiction over an estimated 100,000 businesses that are not subject to the jurisdiction of one of the other agencies responsible for enforcing the G–L–B Act. FTC staff considered many variables affecting the broad spectrum of covered businesses. Some covered businesses may already make the required disclosures in the ordinary course of business. Some may use highly automated means of providing the required disclosures. Others may use low-technology means. The burden estimate also acknowledges that significant start-up burden and attendant costs, such as for determining compliance obligations and developing necessary privacy policies, will be born in the first year that the Rule takes effect. The paperwork burden in subsequent years will be significantly lower. Factoring in start-up costs, the Commission has estimated that the average annual burden during the three year period for which OMB clearance is sought will be 4.03 million burden hours. The estimated annual labor cost associated with these paperwork burdens is $87.3 million. The estimate is also based on the determination that the time required for consumers to respond affirmatively to financial institutions' opt-out notices (be it manually or electronically) will be minimal.

The Commission invites comment that will enable it to:

1. Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility;

2. Evaluate the accuracy of the Commission's estimate of the burden of the proposed collections of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. Minimize the burden of the collections of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Section G. Questions Concerning Comprehensibility of the Rule

The Commission invites your comments on how to make this proposed Rule easier to understand. For example:

- Have we organized the material to suit your needs? If not, how could the material be better organized?
- Are the requirements in the Rule clearly stated? If not, how could the Rule be more clearly stated?
- Does the Rule contain technical language or jargon that is not clear? If not, which language requires clarification?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the Rule easier to understand? If so, what changes to the format would make the Rule easier to understand?
- Would more (but shorter) sections be better? Which ones?
- What else could we do to make the Rule easier to understand?

Section H. Proposed Rule

List of Subjects in 16 CFR Part 313

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

Accordingly, the Commission proposes to amend 16 CFR Ch. I, Subchapter C, by adding a new Part 313 to read as follows:

PART 313—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

Authority: 15 U.S.C. 6804(a).

§ 313.1 Purpose and scope.

(a) *Purpose.* This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution in specified circumstances to provide notice to consumers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 313.9, 313.10, and 313.11.

(b) *Scope.* The rules established by this part apply only to nonpublic personal information about individuals who obtain financial products or services for personal, family or household purposes from the institutions listed in this paragraph. This part does not apply to information about companies or about individuals who obtain financial products or services for business purposes. This part applies to those ''financial institutions'' and ''other persons'' over which the Federal Trade Commission (''Commission'') has enforcement authority pursuant to Section 505(a)(7) of the Gramm-Leach-Bliley Act. An entity is a ''financial institution'' if it is engaged in a financial activity described in Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 211.5(d) and 12 CFR 225.28. The ''financial institutions'' subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the Gramm-Leach-Bliley Act. More specifically, those entities include, but are not limited to, mortgage lenders, ''pay day'' lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, debt collectors, credit counselors and other financial advisors, and tax preparation firms. They are referred to in this part as ''You.'' The ''other persons'' to whom this part applies are third parties that are not financial institutions, but that receive nonpublic personal information from financial institutions with whom they are not affiliated.

§ 313.2 Rule of construction.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part.

§ 313.3 Definitions.

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

(a) *Affiliate* means any company that controls, is controlled by, or is under common control with another company.

(b)(1) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice.

(2) *Examples.* (i) You make your notice reasonably understandable if, to the extent applicable, you:

(A) Present the information contained in the notice in clear, concise sentences, paragraphs and sections;

(B) Use short explanatory sentences and bullet lists, whenever possible;

(C) Use definite, concrete, everyday words and active voice, whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology; and

(F) Avoid boilerplate explanations that are imprecise and readily subject to different interpretations.

(ii) You design your notice to call attention to the nature and significance of the information contained in it if, to the extent applicable, you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read; and

(C) Provide wide margins and ample line spacing.

(iii) If you provide a notice on the same form as another notice or other document, you design your notice to call attention to the nature and significance of the information contained in the notice if you use:

(A) Larger type size(s), boldface or italics in the text;

(B) Wider margins and line spacing in the notice; or

(C) Shading or sidebars to highlight the notice, whenever possible.

(c) *Collect* means to obtain information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information.

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association or similar organization.

(e)(1) *Consumer* means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family or household purposes, and that individual's legal representative.

(2) *Examples.* (i) An individual who applies to you for credit for personal, family or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family or household purposes is a consumer of a financial service, regardless of whether the loan is extended by you or another financial institution.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment or economic advisory services is a consumer of a financial service, regardless of whether you establish a customer relationship.

(iv) An individual who has a credit account with you is a consumer even if you:

(A) Hire an agent to collect on the account;

(B) Sell the rights to service the account; or

(C) Bought the account from the financial institution that originally extended credit.

(v) An individual who makes payments to you on a loan where you own the servicing rights is a consumer. An individual is not your consumer, however, solely because you service the individual's loan on behalf of a financial institution that made the loan to the individual.

(f) *Consumer reporting agency* has the same meaning as in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(g) *Control* of a company means:

(1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

(h) *Customer* means a consumer who has a customer relationship with you.

(i)(1) *Customer relationship* means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family or household purposes.

(2) *Examples.* (i) A consumer has a continuing relationship with you if the consumer:

(A) Has a deposit, credit, trust or investment account with you;

(B) Purchases an insurance product from you;

(C) Holds an investment product through you;

(D) Enters into an agreement or understanding with you whereby you

undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(E) Has a loan that you service where you own the servicing rights;

(F) Enters into a lease of personal property with you;

(G) Obtains financial, investment or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you; or

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a company or financial institution).

(ii) A consumer does not, however, have a continuing relationship with you if:

(A) The consumer only obtains a financial product or service in an isolated transaction such as: withdrawing cash from your ATM; purchasing a cashier's check or money order from you; cashing a check with you; or making a wire transfer through you;

(B) You sell the consumer's loan and do not retain the rights to service that loan; or

(C) You sell the consumer airline tickets, travel insurance or traveler's checks in an isolated transaction.

(j)(1) *Financial institution* means any institution the business of which is engaging in activities that are financial in nature as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) *Example.* An entity is a financial institution if it is significantly engaged in financial activities, such as a retailer that extends credit by issuing its own credit card directly to consumers.

(3) *Financial institution* does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.10 and 313.11.

(iv) A business that only accepts payment by check or cash, or through credit cards issued by others, or through deferred payment or ''lay-away'' plans.

(k)(1) *Financial product or service* means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) *Financial service* includes your evaluation, brokerage or distribution of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(l) *Government regulator* means—

(1) The Board of Governors of the Federal Reserve System;

(2) The Office of the Comptroller of the Currency;

(3) The Board of Directors of the Federal Deposit Insurance Corporation;

(4) The Director of the Office of Thrift Supervision;

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission;

(7) The Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping);

(8) A State insurance authority, with respect to any person domiciled in that insurance authority's State that is engaged in providing insurance; and

(9) The Federal Trade Commission.

(m) *Nonaffiliated third party* means any person except:

(1) Your affiliate; or

(2) A person employed jointly by you and any company that is not your affiliate (but *nonaffiliated third party* includes the other company that jointly employs the person).

[§ 313.3(n-o-p)] Alternative A.

(n)(1) *Nonpublic personal information* means:

(i) Personally identifiable financial information; and

(ii) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information.

(2) *Nonpublic personal information* does not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information.

(3) *Example.* Nonpublic personal information includes any list of individuals' street addresses and telephone numbers that is derived using any information consumers provide to you on an application for a financial product or service.

(o)(1) *Personally identifiable financial information* means any information:

(i) Provided by a consumer to you to obtain a financial product or service from you;

(ii) Resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer, other than publicly available information.

(2) *Examples.* (i) Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you, unless that fact is derived using only publicly available information, such as government real estate records or bankruptcy records;

(D) Other information about your consumer if it is disclosed in a manner that indicates the individual is or has been your consumer;

(E) Any information provided by a consumer or otherwise obtained by you or your agent in connection with collecting on a loan or servicing a loan; and

(F) Information from a consumer report.

(ii) Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; or

(B) A list of names and addresses of consumers to whom you provided a nonfinancial product or service.

(p)(1) *Publicly available information* means any information that is lawfully made available to the general public that is obtained from:

(i) Federal, State or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State or local law.

(2) *Examples.* (i) *Government records.* Publicly available information

contained in government records includes information contained in government real estate records and security interest filings.

(ii) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or an Internet site that is available to the general public without requiring a password or similar restriction.

[§ 313.3(n-o-p)] Alternative B.

(n)(1) *Nonpublic personal information* means:

(i) Personally identifiable financial information; and

(ii) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information.

(2) *Nonpublic personal information* does not include:

(i) Publicly available information, except as provided in paragraph (n)(1)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information.

(3) *Example.* Nonpublic personal information includes any list of individuals' street addresses and telephone numbers that is derived using personally identifiable financial information, such as account numbers.

(o)(1) *Personally identifiable financial information* means any information:

(i) Provided by a consumer to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples.* (i) Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you, unless that fact is derived using only publicly available information, such as government real estate records or bankruptcy records;

(D) Other information about your consumer if it is disclosed in a manner that indicates the individual is or has been your consumer;

(E) Any information provided by a consumer or otherwise obtained by you or your agent in connection with collecting on a loan or servicing a loan; and

(F) Information from a consumer report.

(ii) Personally identifiable financial information does not include a list of names and addresses of customers of an entity that is not a financial institution.

(p)(1) *Publicly available information* means any information that is lawfully made available to the general public from:

(i) Federal, State or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State or local law.

(2) *Examples.* (i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records and security interest filings.

(ii) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or an Internet site that is available to the general public without requiring a password or similar restriction.

(q) *You* means those financial institutions over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

§ 313.4 Initial notice to consumers of privacy policies and practices required.

(a) *When initial notice is required.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:

(1) An individual who becomes your customer, prior to the time that you establish a customer relationship, except as provided in paragraph (d)(2) of this section; and

(2) A consumer, prior to the time that you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 313.10 and 313.11.

(b) *When initial notice to a consumer is not required.* You are not required to provide an initial notice to a consumer under paragraph (a)(1) of this section if:

(1) You do not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by §§ 313.10 and 313.11; and

(2) You do not have a customer relationship with the consumer.

(c) *When you establish a customer relationship.* (1) *General rule.* You establish a customer relationship at the time you and the consumer enter into a continuing relationship.

(2) *Examples.* You establish a customer relationship when the consumer:

(i) Opens a credit card account with you;

(ii) Executes the contract to obtain credit from you, or purchase insurance from you;

(iii) Agrees to obtain financial, economic or investment advisory services from you for a fee;

(iv) Becomes your client for the purpose of your providing credit counseling or tax preparation services, or to obtain career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a company or financial institution);

(v) Provides any personally identifiable financial information to you in an effort to obtain a mortgage loan through you; or

(vi) Makes his or her first payment to you on a loan account for which you have obtained the servicing rights.

(d) *How to provide notice.* (1) *General rule.* You must provide the privacy notice required by paragraph (a) of this section so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form.

(2) *Exceptions to allow subsequent delivery of notice.* You may provide the initial notice required by paragraph (a)(1) of this section within a reasonable time after you establish a customer relationship if:

(i) You purchase a loan from another financial institution and the customer of that loan does not have a choice about your purchase; or

(ii) You and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice thereafter.

(3) *Oral description of notice insufficient.* You may not provide the initial notice required by paragraph (a) of this section solely by orally explaining, either in person or over the telephone, your privacy policies and practices.

(4) *Retention or accessibility of initial notice for customers.* For customers only, you must provide the initial notice required by paragraph (a)(1) of this section so that it can be retained or obtained at a later time by the customer, in a written form or, if the customer agrees, in electronic form.

(5) *Examples.* (i) You may reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:

(A) Hand-deliver a printed copy of the notice to the consumer;

(B) Mail a printed copy of the notice to the last known address of the consumer;

(C) For the consumer who conducts transactions electronically, post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service; or

(D) For an isolated transaction with the consumer, such as an ATM transaction, post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

(ii) You may *not*, however, reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:

(A) Only post a sign in your office or generally publish advertisements of your privacy policies and practices; or

(B) Send the notice via electronic mail to a consumer who obtains a financial product or service with you in person or through the mail and who does not agree to receive the notice electronically.

(iii) You provide the initial privacy notice to the customer so that it can be retained or obtained at a later time if you:

(A) Hand-deliver a printed copy of the notice to the customer;

(B) Mail a printed copy of the notice to the last known address of the customer upon request of the customer; or

(C) Maintain the notice on a web site (or a link to another web site) for the customer who obtains a financial product or service electronically and who agrees to receive the notice electronically.

§ 313.5 Annual notice to customers required.

(a) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of twelve consecutive months during which that relationship exists.

(b) *How to provide notice.* You must provide the annual notice required by paragraph (a) of this section to a customer using a means permitted for providing the initial notice to that customer under § 313.4(d).

(c) (1) *Termination of customer relationship.* You are not required to provide an annual notice to a customer with whom you no longer have a continuing relationship.

(2) *Examples.* You no longer have a continuing relationship with an individual if:

(i) In the case of a closed-end loan, the consumer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;

(ii) In the case of a credit card relationship or other open-end credit relationship, you no longer provide any statements or notices to the consumer concerning that relationship or you sell the credit card receivables without retaining servicing rights; or

(iii) For other types of relationships, you have not communicated with the consumer about the relationship for a period of twelve consecutive months, other than to provide annual notices of privacy policies and practices.

§ 313.6 Information to be included in initial and annual notices of privacy policies and practices.

(a) *General rule.* The initial and annual notices that you provide about your privacy policies and practices under §§ 313.4 and 313.5 must include each of the following items of information:

(1) The categories of nonpublic personal information about your consumers that you collect;

(2) The categories of nonpublic personal information about your consumers that you disclose;

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your consumers, other than those parties to whom you disclose information under §§ 313.10 and 313.11;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 313.10 and 313.11;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 313.9 (and no other exception applies to that disclosure), a separate description of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the right under § 313.8(a) of the consumer to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;

(7) Any disclosures that you make under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates); and

(8) Your policies and practices with respect to protecting the confidentiality, security and integrity of nonpublic personal information.

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information about a consumer to third parties as authorized under §§ 313.10 and 313.11, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 313.4 and 313.5. When describing the categories with respect to those parties, you are only required to state that you make disclosures to other nonaffiliated third parties as permitted by law.

(c) *Future disclosures.* Your notice may include:

(1) Categories of nonpublic personal information that you reserve the right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom you reserve the right in the future to disclose, but to whom you do not currently disclose, nonpublic personal information.

(d) *Examples.* (1) *Categories of nonpublic personal information that you collect.* You adequately categorize the nonpublic personal information you collect if you categorize it according to the source of the information, such as application information, information about transactions (such as information regarding your deposit, loan, or credit card account), and consumer reports.

(2) *Categories of nonpublic personal information you disclose.* You adequately categorize nonpublic personal information you disclose if you categorize it according to source, and provide illustrative examples of the content of the information. These might include application information, such as assets and income; identifying information, such as name, address, and social security number; and transaction information, such as information about account balance, payment history,

parties to the transaction, and credit card usage; and information from consumer reports, such as a consumer's creditworthiness and credit history. You do not adequately categorize the information that you disclose if you use only general terms, such as transaction information about the consumer.

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.* You adequately categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about consumers if you identify the types of businesses that they engage in. Types of businesses may be described by general terms only if you use illustrative examples of significant lines of business. For example, you may use the term ''financial products or services'' if you include appropriate examples of significant lines of businesses, such as consumer banking, mortgage lending, life insurance or securities brokerage. Likewise, you may refer to ''retail products'' if you include examples such as clothing. household furnishings, and health-related items, or to ''magazine subscription products'' if you include such examples as health-related or investment-related publications. You also may categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about consumers using more detailed categories.

(4) *Simplified notices.* If you do not disclose, and do not intend to disclose, nonpublic personal information to affiliates or nonaffiliated third parties, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), and (b) of this section.

(5) *Confidentiality, security and integrity.* You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if you explain who has access to the information and the circumstances under which the information may be accessed. You describe your policies and practices with respect to protecting the integrity of nonpublic personal information if you explain measures you take to protect against reasonably anticipated threats or hazards. You are not required to describe technical information about the safeguards you use.

§ 313.7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.

(a)(1) *Conditions for disclosure.* Except as otherwise authorized in this part, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:

(i) You have provided to the consumer an initial notice as required under § 313.4;

(ii) You have provided to the consumer an opt out notice as required in § 313.8;

(iii) You have given the consumer a reasonable opportunity, before the time that you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 313.9, 313.10 and 313.11.

(3) *Examples of reasonable opportunity to opt out.* (i) *By mail.* You provide a consumer with whom you have a customer relationship with a reasonable opportunity to opt out if you mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer a reasonable period of time, such as 30 days, to opt out.

(ii) *Isolated transaction with consumer.* For an isolated transaction, such as the purchase of a cashier's check by a consumer, you provide a reasonable opportunity to opt out if you provide the consumer with the required notices at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

(b) *Application of opt out to all consumers and all nonpublic personal information.* (1) This section applies regardless of whether you and the consumer have established a customer relationship.

(2) Unless you comply with this section, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that you have collected, regardless of whether you collected it before or after receiving the direction to opt out from the consumer.

(c) *Partial opt out.* You may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

§ 313.8 Form and method of providing opt out notice to consumer.

(a)(1) *Form of opt out notice.* You must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under § 313.7(a)(1). The notice must state:

(i) That you disclose or reserve the right to disclose nonpublic personal information about your consumer to a nonaffiliated third party;

(ii) That the consumer has the right to opt out of that disclosure; and

(iii) A reasonable means by which the consumer may exercise the opt out right.

(2) *Examples.* (i) You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose to nonaffiliated third parties as described in § 313.6 and state that the consumer can opt out of the disclosure of that information.

(ii) You provide a reasonable means to exercise an opt out right if you:

(A) Designate check-off boxes in a prominent position on the relevant forms with the opt out notice and clearly identify where to send the notice;

(B) Include a detachable form and self-addressed stamped envelope together with the opt out notice;

(C) Provide an electronic means to opt out, such as a form that can be sent via electronic mail or a process at your Web site, if the consumer agrees to the electronic delivery of information; or

(D) Designate a toll-free number that the consumer can call to opt out.

(b) *How to provide opt out notice.* (1) *Delivery of notice.* You must provide the opt out notice required by paragraph (a) of this section in a manner so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form. If you and the consumer orally agree to enter into a customer relationship, you may provide the opt out notice required by paragraph (a) of this section within a reasonable time thereafter if the consumer agrees.

(2) *Oral description of opt out right insufficient.* You may not provide the opt out notice solely by orally explaining, either in person or over the telephone, the right of the consumer to opt out.

(3) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 313.4.

(4) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice at a later time than required for the initial notice in accordance with

§ 313.4, you must also include a copy of the initial notice in writing or, if the consumer agrees, in an electronic form with the opt out notice.

(c) *Notice of change in terms.* (1) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to the consumer under § 313.4, unless—

(i) You have provided to the consumer a revised notice that accurately describes your policies and practices;

(ii) You have provided to the consumer a new opt out notice;

(iii) You have given the consumer a reasonable opportunity, before the time that you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) *How to provide notice of change in terms.* You must provide the revised notice of your policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under § 313.4(d) or paragraph (b) of this section, respectively.

(3) *Examples.* (i) Except as otherwise permitted by §§ 313.9, 313.10 and 313.11, a change-in-terms notice is required if you—

(A) Disclose a new category of nonpublic personal information to any nonaffiliated third party; or

(B) Disclose nonpublic personal information to a new category of nonaffiliated third party.

(ii) A change-in-terms notice is not required if you disclose nonpublic personal information to a new nonaffiliated third party that is adequately described by your prior notice.

(d) *Continuing right to opt out.* A consumer may exercise the right to opt out at any time, and you must comply with the consumer's direction as soon as reasonably practicable.

(e) *Duration of consumer's opt out direction.* A consumer's direction to opt out under this section is effective until revoked by the consumer in writing or, if the consumer agrees, in electronic form.

§ 313.9 Exception to opt out requirements for service providers and joint marketing.

(a) *General rule.* The opt out requirements in §§ 313.7 and 313.8 do not apply when you provide nonpublic personal information about a consumer to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(1) Provide the initial notice in accordance with § 313.4; and

(2) Enter into a contractual agreement with the third party that:

(i) Requires the third party to maintain the confidentiality of the information to at least the same extent that you must maintain that confidentiality under this part; and

(ii) Limits the third party's use of information you disclose solely to the purposes for which the information is disclosed or as otherwise permitted by §§ 313.10 and 313.11.

(b) *Service may include joint marketing.* The services performed for you by a nonaffiliated third party under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.

(c) *Definition of joint agreement.* For purposes of this section, *joint agreement* means a written contract pursuant to which you and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

§§ 313.9 313.10 Exceptions to notice and opt out requirements for processing and servicing transactions.

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 313.4(a)(2), the opt out in §§ 313.7 and 313.8, and service providers and joint marketing in § 313.9 do not apply if you disclose nonpublic personal information:

(1) As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer;

(2) To service or process a financial product or service requested or authorized by the consumer;

(3) To maintain or service the consumer's account with you, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(4) In connection with a proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer.

(b) *Necessary to effect, administer, or enforce a transaction* means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the financial service or financial product;

(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(iii) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;

(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;

(v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or State law;

(vi) In connection with settling a transaction, including:

(A) The authorization, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(B) The transfer of receivables, accounts or interests therein; or

(C) The audit of debit, credit or other payment information.

§ 313.11 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice to consumers in § 313.4(a)(2), the opt out in §§ 313.7 and 313.8, and service providers and joint marketing in § 313.9 do not apply when you disclose nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2)(i) To protect the confidentiality or security of your records pertaining to the consumer, service, product or transaction;

(ii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;

(iii) For required institutional risk control or for resolving consumer disputes or inquiries;

(iv) To persons holding a legal or beneficial interest relating to the consumer; or

(v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*), to law enforcement agencies (including government regulators), self-regulatory organizations, or for an investigation on a matter related to public safety;

(5)(i) To a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), or

(ii) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(7)(i) To comply with Federal, State or local laws, rules and other applicable legal requirements;

(ii) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by Federal, State or local authorities; or

(iii) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance or other purposes as authorized by law.

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to you for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 313.8(d).

§ 313.12 Limits on redisclosure and reuse of information.

(a) *Limits on your redisclosure and reuse.* (1) Except as otherwise provided in this part, if you receive nonpublic personal information about a consumer from a nonaffiliated financial institution, you must not, directly or through an affiliate, disclose the information to any other person that is not affiliated with either the financial institution or you, unless the disclosure would be lawful if the financial institution made it directly to such other person.

(2) You may use nonpublic personal information about a consumer that you receive from a nonaffiliated financial institution in accordance with an exception under §§ 313.9, 313.10 or 313.11 only for the purpose of that exception.

(b) *Limits on redisclosure and the reuse by other persons.* (1) Except as otherwise provided in this part, if you disclose nonpublic personal information about a consumer to a nonaffiliated third party, that party must not, directly or through an affiliate, disclose the information to any other person that is a nonaffiliated third party of both you and that party, unless the disclosure would be lawful if you made it directly to such other person.

(2) A nonaffiliated third party may use nonpublic personal information about a consumer that it receives from you in accordance with an exception under §§ 313.9, 313.10 or 313.11 only for the purpose of that exception.

§ 313.13 Limits on sharing of account number information for marketing purposes.

You must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

§ 313.14 Protection of Fair Credit Reporting Act.

Nothing in this part shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), and no inference shall be drawn on the basis of the provisions of this part regarding whether information is transaction or experience information under section 603 of that Act.

§ 313.15 Relation to state laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation in effect in any State, except to the extent that such state statute, regulation, order or interpretation is inconsistent with the provisions of this part, and then only to the extent of the inconsistency.

(b) *Greater protection under state law.* For purposes of this section, a State statute, regulation, order or interpretation is not inconsistent with the provisions of this part if the protection such statute, regulation, order or interpretation affords any consumer is greater than the protection provided under this part, as determined by the Commission on its own motion or upon the petition of any interested party, after consultation with the applicable government regulator or other authority.

§ 313.16 Effective date; transition rule.

(a) *Effective date.* This part is effective November 13, 2000.

(b) *Notice requirement for consumers who were your customers on the effective date.* No later than thirty days after the effective date of this part, you must provide an initial notice, as required by § 313.4, to consumers who were your customers on the effective date of this part.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 00–4881 Filed 2–29–00; 8:45 am]

BILLING CODE 6750–01–P