Federal Register

Wednesday,
May 24, 2000

Part III

Federal Trade Commission

16 CFR Part 313

Privacy of Consumer Financial Information; Final Rule

FEDERAL TRADE COMMISSION

16 CFR Part 313

Privacy of Consumer Financial Information

AGENCY: Federal Trade Commission.

ACTION: Final Rule.

SUMMARY: The Federal Trade Commission (the ''Commission'' or ''FTC'') is publishing a final privacy rule, as required by section 504(a) of the Gramm-Leach-Bliley Act, Pub. L. 106-102 (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. Section 504 of the Act requires the Commission and other federal regulatory agencies to issue regulations as may be necessary to implement 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 prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution satisfies various disclosure and opt-out requirements and the consumer has not elected to opt out of the disclosure. This final rule implements the requirements outlined above.

EFFECTIVE DATE: This rule is effective November 13, 2000. Full compliance is required by July 1, 2001.

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) 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. 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 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.[1] Title V also requires the Commission, along with the Federal banking agencies [2] and other Federal regulatory authorities,[3] after consulting with representatives of State insurance authorities designated by the National Association of Insurance Commissioners (NAIC), 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 Federal agencies are sometimes referred to collectively in this document as the ''Agencies'' (or ''other Agencies'' when excluding the Commission).

The Agencies are all issuing final rules to implement Subtitle A that are consistent and comparable to the extent possible, as is required by the statute.

Section B. Overview of Comments Received

On March 1, 2000, the Commission published a notice of proposed rulemaking (the proposal or proposed rule) in the **Federal Register** (65 FR 11174). The other Agencies published their proposed rules on different dates.[4] The Commission received a total of 640 comments, and the other Agencies collectively received a total of 8,337 comments in response to the various proposed rules. Many commenters sent the same letter to multiple Agencies. Many of the comments were from individuals, virtually all of whom encouraged the Agencies to provide greater protection of individuals' financial privacy. Many individuals noted their concerns generally about the loss of privacy and the receipt of unwanted solicitations by marketers. A large number of individuals also requested the Agencies to support legislation that the commenters believe would provide additional protections.

The Agencies also received several letters from members of Congress. In two letters signed by several members of the House of Representatives, the Agencies were encouraged to exercise their rulemaking authority to provide greater protections than provided in the Act. Other Representatives requested, in separate letters, that some other Agencies (a) create a limited exception to the prohibition against the sharing of account numbers for marketing purposes and (b) ensure that social security numbers are considered ''nonpublic personal information.''

The NAIC submitted a comment on behalf of the State insurance authorities that generally supported the Agencies' proposed rule. The NAIC also proposed various measures to provide greater protections for consumers, such as specifying more convenient means to exercise the right to opt out of the disclosure of information. The NAIC further advised the Agencies to clarify the boundary of Federal and State jurisdiction over privacy regulations and ensure that the financial privacy rules under the Act are compatible with the privacy rules relating to medical information that are to be issued by the Secretary of the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPPA) of 1996.[5]

Other comments were received from consumer groups and others advocating that the Agencies extend privacy protections in a number of ways, such as by requiring (a) financial institutions to provide consumers with access to their information maintained by the institutions and the opportunity to correct errors, (b) more detailed disclosures of the information collected and disclosed, and (c) disclosures of a financial institution's privacy policies and practices earlier in the process of establishing a customer relationship. A letter signed by 33 State Attorneys General urged some other Agencies to add certain consumer protections to the disclosure requirements and to the

[1] The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 *et seq*, provides no limitation on communication by an entity solely of its own ''transactions or experiences'' with the consumer (*e.g.*, the individual's account history). However, it limits the reporting of information obtained from other sources, such as consumer application information or credit report information. 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 by the FCRA, because the institution likely would become a consumer reporting agency subject to its restrictions on reporting of information to third parties.

[2] Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Secretary of the Treasury.

[3] National Credit Union Administration (NCUA) and Securities and Exchange Commission (SEC).

[4] Those proposed rules, which were consistent and comparable with the proposals published by the Commission, appeared in the **Federal Register** at 65 FR 8770 (Feb. 22, 2000) (OCC, FRB, FDIC, and OTS jointly), 65 FR 10988 (Mar. 1, 2000) (NCUA), and 65 FR 12354 (Mar. 8, 2000) (SEC).

[5] These proposed regulations were published for comment at 64 FR 59918 (Nov. 3, 1999).

provision permitting financial institutions to enter into joint marketing agreements.

Most of the remaining comments were from businesses concerned about the Act, and their representatives. This included not only creditors of various types, but also representatives of the health care industry, retail merchants, insurance companies, securities firms, private investigators, debt collection agencies, consumer reporting agencies, institutions of higher education, tax professionals, and others. These commenters offered a large number of suggested changes, with the most commonly advanced suggestions including: an extension of the effective date of the rule; an amendment to the definition of ''nonpublic personal information'' to focus more narrowly on ''financial'' information; a streamlining of information required in the initial and annual disclosures; a clarification of how one or more of the statutory exceptions operate; an exclusion from, or clarification of, the definitions of ''consumer'' and ''customer'' in various contexts; and the addition of flexibility to provide initial notices at some point other than ''prior to'' the time a customer relationship is established.

The Commission has made some modifications to its proposed rule in light of the comments received. These comments, and the Commission's responses thereto, are discussed in the following section-by-section analysis. Following the section-by-section analysis, the Commission has provided guidance for certain institutions in order to provide additional direction on how these institutions may comply with the rule and avoid unnecessary burden.

Section C. Section-by-Section Analysis

As an initial matter, the Commission notes that the final rule, unlike the proposal, presents the various sections in subparts that consist of related sections. This change was made to group related concepts together and thereby make the rule easier to follow. A derivation table is included following this preamble to assist readers in locating provisions as set out in the Commission proposal. The Commission has also added an Appendix to the final rule, setting out example disclosure clauses for financial institutions to consider.

Section 313.1 Purpose and Scope

Purpose. Paragraph (a) of this section states that the rule is intended to require a financial institution to provide notice to customers about its privacy policies and practices; to describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and to provide a method for consumers to prevent a financial institution from disclosing that information to certain nonaffiliated third parties by ''opting out'' of that disclosure, subject to various exceptions as stated in the rule. No significant comments addressed this provision, and the Commission made no substantive change to this section.

Scope. Paragraph (b) sets out the scope of the rule, and tracks the enforcement role assigned to the Commission by section 505(a)(7) of the G-L-B Act. It 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 section 509(3) of the G-L-B Act defines very broadly 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,[6] but also those activities that the Federal Reserve Board has found to be either closely related to banking,[7] or usual in connection with the transaction of banking or other financial operations abroad,[8] by regulation (or order or interpretation) ''in effect on the date of the enactment of the Gramm-Leach-Bliley Act.''[9] Section 313.1(b) also lists some examples of ''financial institutions'' subject to Commission jurisdiction under the Act. Finally, this part notes that 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 section 502(c) of the G-L-B Act (''Limits on Reuse of Information''), which imposes restrictions on recipients of such information as set forth in 16 CFR 313.11, *infra*.

Many industry commenters suggested revising the ''financial institution'' definition set forth in § 313.3(k) to narrow the scope to only those businesses that engage in traditional financial activities, arguing that Congress did not intend to cover businesses that conducted no such activities. On the other side, consumer commenters vigorously defended the broad scope, contending that the need to protect personal financial data extends beyond traditional financial institutions and that Congress intended to regulate a wide range of businesses that provide ''financial'' services to consumers when it enacted this statute. The G-L-B Act clearly covers more than parties in the credit, insurance, or securities industries; rather, an entity is a ''financial institution'' if it engages in any activity that the Board has determined to be a ''financial activity.''

[6] 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.''

[7] Section 4(k)(4)(F). The Board's list of such activities is found in 12 CFR 225.28 and 12 CFR 225.86(a). The latter subsection was added as an interim rule published by the Board in the **Federal Register** upon enactment of the G-L-B Act (65 FR 14433; Mar. 14, 2000), subject to revision after a public comment period ending on May 12, 2000. The activities listed in 12 CFR 225.28 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.

[8] 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 Section 4(k)(4)(G) activity that (i) a bank holding company may engage in outside of the United States; and (ii) the Board has determined 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) and 12 CFR 225.86(b). The latter subsection was added as an interim rule published by the Board in the **Federal Register** upon enactment of the G-L-B Act (65 FR 14433; Mar. 14, 2000), subject to revision following a public comment period ending on May 12, 2000. The activities listed in 12 CFR 211.5(d) 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.

[9] Section 4(k)(4)(G) uses ''*day before the* date of'' rather than ''date of'' in the quoted phrase.

After a careful review of the comments received, the Commission finds no sound rationale for fundamentally revising the scope of the rule. Therefore, the Commission continues to interpret the act as written and has made no broad change to 16 CFR 313.1(b) in that regard.[10] However, as the Commission noted when it proposed this rule and repeats hereafter, some businesses that are technically ''financial institutions'' will have no disclosure obligations under the Act.[11] Furthermore, as is evident from the discussion of the term ''customer relationship'' that is defined in 16 CFR 313.3(i), many others will have only limited duties because they will not establish such relationships or they will be of very short duration.

Several commenters requested that the Commission clarify how its rule applies to insurance companies. The Commission notes that section 505 of G-L-B Act, which sets out the enforcement authority of the Agencies, explicitly commits the enforcement jurisdiction over ''persons engaged in providing insurance'' to state insurance authorities, thus excluding them from the Commission's authority (and, by operation of section 504(a)(1) of the G-L-B Act, from the Commission's rulemaking authority).

Several other commenters asked that the final rule state that certain transactions that are exempt from the coverage of the Truth in Lending Act (TILA; 15 U.S.C. 1601 *et seq.*) and Regulation Z (Reg. Z, 12 CFR part 226) also be treated as beyond the scope of the privacy rule. TILA and Reg. Z, which impose disclosure requirements on credit extended to consumers under certain circumstances, exempt several transactions, including those involving business, commercial, or agricultural credit. 15 U.S.C. 1603(1); 12 CFR 226.3(a). The Commission agrees that transactions that fit within the business, commercial, and agricultural exemptions from TILA and Reg. Z for these types of credit also would fall outside the scope of the privacy rule, and has amended § 313.1(b) accordingly.[12]

Several comments suggested that the rule should not apply to entities that must comply with regulations issued by the HHS that implement the HIPAA. Given the broad definition of ''financial institution'' under the G-L-B Act, certain entities are subject to these privacy rules as well as rules promulgated under HIPAA regarding appropriate handling of protected health information. Accordingly, financial institutions may be covered both by this privacy rule and by the regulations promulgated by HHS under the authority of sections 262 and 264 of HIPAA once those regulations are finalized. Based on the proposed HIPAA rules, it appears likely that there will be areas of overlap between HIPAA and financial privacy rules. For instance, under the proposed HIPAA regulations, consumers must provide affirmative authorization before a covered institution may disclose medical information in certain instances, whereas under the financial privacy rules, institutions need only provide consumers with the opportunity to opt out of disclosures. In this case, the Agencies anticipate that compliance with the affirmative authorization requirement, consistent with the procedures required under HIPAA, would satisfy the opt out requirement under the financial privacy rules. After HHS publishes its final rules, the Commission and other Agencies will consult with HHS to avoid the imposition of duplicative or inconsistent requirements.

The Commission also received several comments from colleges and universities and their representatives requesting that institutions of higher education be excluded from the definition of financial institution. The Commission disagrees with those commenters who suggested that colleges and universities are not financial institutions. Many, if not all, such institutions appear to be significantly engaged in lending funds to consumers. However, such entities are subject to the stringent privacy provisions in the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, which govern the privacy of educational records, including student financial aid records. The Commission has noted in its final rule, therefore, that institutions of higher education that are complying with FERPA to protect the privacy of their student financial aid records will be deemed to be in compliance with the Commission's rule.

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. As noted in the proposal, these examples are not intended to be exhaustive; rather, they are intended to provide guidance about how the rule would apply in specific situations.

Commenters generally agreed that examples are helpful in clarifying how the rule will work in specific circumstances and suggested that the Commission should include more examples. Many commenters requested that the Commission provide examples of model disclosures. Commenters also generally agreed that it is useful to state that the list of examples is not intended to be exhaustive, and that compliance with one of the examples would be deemed compliance with the regulation. A few commenters suggested that the regulation state that a financial institution is not obligated to comply with an example but has the latitude to comply with the general rule in other ways. Others stated that the examples ought to be identical in each privacy regulation adopted by the Agencies. The Commission also received comments suggesting that the Commission defer to the expertise of other agencies when considering application of its rule to entities such as credit unions or investment advisors under its jurisdiction.

The Commission believes that more examples would be helpful and has included additional examples in appropriate places throughout the rule. The Commission has also provided sample clauses in Appendix A to the rule to aid financial institutions in their drafting of privacy notices. The sample clauses are provided to illustrate the level of detail the Commission believes is appropriate. The Commission cautions financial institutions against relying on the sample clauses without determining the relevance or appropriateness of the disclosure for their operations. The Commission has used statutory terms, such as ''nonpublic personal information'' and ''nonaffiliated third parties,'' in the sample clauses to convey generally the subject of the clauses. However, a financial institution that uses these terms must provide sufficient information to enable consumers to understand what these terms mean in the context of the institution's notices. Moreover, the Commission notes that, in providing the sample disclosures, the Commission is addressing solely the

[10] However, as discussed in the definition of ''financial institution'' in § 313.3(k), the Commission has retained its interpretation that an institution is covered only if it is ''significantly engaged'' in such activities.

[11] ''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.' '' 65 Fed. Reg. 11174, 11177 (Mar. 1, 2000).

[12] Thus, creditors may look at how this exemption is applied under Reg. Z for guidance on the scope of covered transactions under the privacy rule. It should be noted, however, that TILA exempts several other types of transactions that would be covered under the privacy rule if they are for the purpose of an individual obtaining a financial product or service as that term is defined in the privacy regulation. *See* 15 U.S.C. 1603 (2) and (3).

level of detail required and is not attempting to provide guidance on issues such as type size, margin width, ''clear and conspicuous'' generally, and so on.

The rule does not contain a statement regarding a financial institution's ability to comply with the rule in ways other than as suggested in the examples, but does provide that the examples are not exclusive. The rule also states that compliance with the examples will constitute compliance with the rule. The Commission believes that, when read together, these provisions give financial institutions sufficient flexibility to comply with the regulation but also sufficient guidance about the use of examples.

The Commission understands that the NCUA and SEC have issued, or will issue, final rules with examples that are tailored to entities under their jurisdiction. Therefore, the Commission has stated in § 313.2 that compliance by non-federally insured credit unions with credit union examples in the NCUA rule will constitute compliance with the Commission's rule. Similarly, compliance by interstate securities broker-dealers and investment advisers that are not registered with the SEC with applicable examples in the SEC rule will constitute compliance with the Commission's rule.

Section 313.3 Definitions

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

The Commission received comparatively few comments in response to this definition. A few commenters requested that the final rule state that a credit union service organization will be deemed to be an affiliate of every credit union that has an interest in it. The Commission has declined to adopt this suggestion. If the relationship between a credit union and a credit union service organization satisfies the test for affiliation set out in the statute and regulation, then an affiliation exists.

In light of the comparatively few comments received and the nature of those comments, the Commission adopts the definition of ''affiliate'' as proposed.

b. *Clear and conspicuous.* Under the proposed rule, various notices must be ''clear and conspicuous.'' The proposed rule defines this term to mean that the notice must be reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. The proposal did not mandate the use of any particular technique for making the notices clear and conspicuous, but provided examples of how a notice may be made clear and conspicuous. As noted in the preamble to the proposed rule, each financial institution retains the flexibility to decide for itself how best to comply with this requirement.

The Commission received a large number of comments on this proposed definition. Some commenters favored adopting the definition as proposed, with some of these advocating that the final rule add a requirement that disclosures must be on a separate piece of paper in order to ensure that they will be conspicuous. Others stated that the definition was unnecessary, given the experience financial institutions have in complying with requirements that disclosures mandated by other laws be clear and conspicuous. Several commenters made the related point that the rule proposed is inconsistent with requirements in other consumer protection regulations such as Reg. Z and the Truth in Savings regulation (Regulation DD, 12 CFR part 230), which require only that a disclosure be reasonably understandable. Many of these commenters expressed concern that the examples would invite litigation because of ambiguities inherent in terms used in the examples in the proposed rule such as ''ample line spacing,'' ''wide margins,'' and ''explanations * * * subject to different interpretations.'' A few commenters questioned how the requirement would work in a document that contains several disclosures that each must be clearly and conspicuously disclosed, while others raised questions about how a disclosure may be clear and conspicuous on a web site. These comments are addressed below.

New standard for ''clear and conspicuous'' The Commission recognizes that the proposed definition articulates the concept of ''clear and conspicuous'' in ways perhaps not familiar to some commenters. However, the Commission included the phrase ''designed to call attention to the nature and significance of the information contained'' to provide added meaning to the term ''conspicuous.'' The Commission believes that this standard, when coupled with the existing standard requiring that a disclosure be readily understandable, likely will result in notices to consumers that communicate effectively the information needed by consumers to make an informed choice about the privacy of their information, including whether to transact business with a financial institution.

The standard for clear and conspicuous adopted by the Commission in this rulemaking applies solely to disclosures required under the privacy rules. Disclosures governed by other rules requiring clear and conspicuous disclosures (such as Reg. Z) are beyond the scope of this rulemaking.

Examples of ''clear and conspicuous'' The Commission recognizes that many of the examples require judgment in their application. The Commission believes, however, that more prescriptive examples, while perhaps easier to conform to, likely would result in requirements that would be inappropriate in a given circumstance. To avoid this result, the examples provide generally applicable guidance about ways in which a financial institution may make a disclosure clear and conspicuous. The Commission notes that the examples of how to make a disclosure clear and conspicuous are not mandatory. A financial institution must decide for itself how best to comply with the general rule and may use techniques not listed in the examples. To address these concerns, the Commission has incorporated several of the commenters' suggestions for ways to make the guidance more helpful.

Combination of several ''clear and conspicuous'' notices. A document may combine several disclosures that each must be clear and conspicuous. The final rule provides an example, in § 313.3(b)(2)(ii)(E), of how a financial institution may make disclosures conspicuous, including disclosures on a combined notice. In order to avoid the potential conflicts envisioned by several commenters between two different requirements, the final rule does not mandate precise specifications for how various disclosures must be presented.

Because the Commission believes that privacy disclosures may be clear and conspicuous when contained in a document containing other disclosures, the rule does not mandate that disclosures be provided on a separate piece of paper. Such a requirement is not necessary and would significantly increase the burden on financial institutions. Moreover, it would not necessarily provide the most effective notice in all circumstances.

Disclosures on web pages. Several commenters requested guidance on how they may clearly and conspicuously

disclose privacy-related information on their Internet sites. The Commission recognizes that disclosures over the Internet present some issues that will not arise in paper-based disclosures. There may be web pages within a financial institution's website that consumers may view in a different order each time they access the site, aided by hypertext links. Depending on the customer hardware and software used to access the Internet, some web pages may require consumers to scroll down to view the entire page. To address these issues, the Commission has included a statement in the example in § 313.3(b)(2)(iii) concerning Internet disclosures informing financial institutions that they may comply with the rule if they use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice. In addition, a financial institution is to place either a notice or a conspicuous link on a page frequently accessed by consumers, such as a page on which transactions are conducted.

Given current technology, there are a range of approaches a financial institution could take to comply with the rule. For example, a financial institution could use a dialog box that pops up to provide the disclosure before a consumer provides information to the institution. Another approach would be a simple, clearly labeled graphic located near the top of the page or in close proximity to the financial institution's logo, directing the customer, through a hypertext link or hotlink, to the privacy disclosures on a separate web page.

For the reasons advanced above, the Commission has adopted the definition of ''clear and conspicuous,'' with the changes previously described and with certain other changes intended to make the definition easier to apply.

c. *Collect.* The statute requires a financial institution to include in its initial and annual notices a disclosure of the categories of nonpublic personal information that the institution collects. The proposal defined ''collect'' to mean obtaining any information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information. This definition was included to provide guidance about the information that a financial institution must include in its notices and to clarify that the obligations arise regardless of whether the financial institution obtains the information from a consumer or from some other source.

Commenters suggested that the final rule treat information that is not organized and retrievable in an automated fashion as not ''collected.'' This approach would exclude separate documents not included in a file. The Commission disagrees that information should not be deemed to be collected simply because it is not retrievable in an automated fashion. The Commission believes that the method of retrieval is irrelevant to whether information should be protected under the rule. The Commission agrees, however, that the scope of the regulation should be refined, and has changed the definition of ''collect'' by using language taken from the Privacy Act of 1974 (5 U.S.C. 552a).

Other commenters requested that the rule clarify that information that is received by a financial institution but then immediately passed along without otherwise disclosing, using, or maintaining a copy of the information is not ''collected'' as this term is used in the final rule. The Commission believes that merely receiving information without maintaining it would not be ''collecting'' the information. The final rule reflects this by stating that the information must be organized or retrievable by the financial institution. Otherwise, the definition of ''collect'' is adopted as proposed.

d. *Company.* The proposal defined ''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.

The Commission received no substantive comments on this proposed definition.[13] Accordingly, the Commission adopts the definition of ''company'' as proposed.

e. *Consumer.* The G-L-B Act distinguishes ''consumers'' from ''customers'' for purposes of the notice requirements imposed by the Act. A financial institution is required to give a ''consumer'' the notices required under Title V only if the institution intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party for purposes other than as permitted by section 502(e) of the statute (as implemented by §§ 313.14 and 313.15). 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.

The proposed rule defined ''consumer'' to mean an individual (and his or her legal representative) who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes. Because ''financial product or service'' is defined to include the evaluation by a financial institution of an application to obtain a financial product or service (*see* further discussion of this point, below), a person becomes a consumer even if the application is denied or withdrawn. An individual also would be deemed to be a consumer (as well as a customer) of a financial institution that purchases the individual's account from some other institution.

The Commission received a large number of comments on this proposed definition, raising questions about how the definition would apply in a variety of situations. These comments are addressed below.

Distinction between ''consumer'' and ''customer.'' While many agreed with the distinction drawn in the proposal between ''consumer'' and ''customer,'' a few commenters suggested that no distinction between ''consumer'' and ''customer'' should be made, given that, in these commenters'' views, the statute appears to use the terms interchangeably. The Commission believes, however, that the distinction was deliberate and that the rule should implement it accordingly. A plain reading of the statute supports the conclusion that Congress created one set of protections for anyone who obtains a financial product or service (*i.e.,* who receives a financial institution's privacy policy and opt out notice only if a financial institution intends to disclose nonpublic personal information to nonaffiliated third parties), and an additional set of protections for anyone who establishes a relationship of a more lasting nature than an isolated transaction with a financial institution (*i.e.,* who gets a notice of the institution's privacy policy at the time of establishing a customer relationship, and annual notices as appropriate thereafter). Because the statute tailors the notice requirements to the type of relationship an individual has with a financial institution, that distinction is preserved in the rule.

Applicants as consumers. Many of the comments received by the Commission concerning the proposed definition of ''consumer'' disagreed that someone should be deemed a consumer of a financial institution simply by

[13] However, the Commission did receive a few comments asking that sole proprietors be excluded from the definitions of both ''company'' and ''financial institution.'' Those comments are discussed in the context of § 313.3(k).

virtue of the institution evaluating an application. These commenters maintained that the individual has not obtained a financial product or service, as is required by the statutory definition of ''consumer.'' The Commission believes that the better reading of the G-L-B Act is that an individual has obtained a financial product or service when a financial institution evaluates information provided to the financial institution for the purpose of the individual obtaining some other financial product or service. Financial institutions frequently provide a range of services in connection with the delivery of a financial product. Included within these will be the evaluation by the financial institution of information provided by an individual. In certain instances, such as when an individual is shopping for the best rate on a mortgage loan or the lowest premium for an insurance policy, that evaluation may be the sole financial product or service obtained. In other instances, the evaluation may be one of several services provided that lead up to the eventual establishment of a customer relationship. In either case, the individual will have obtained a financial product or service from the financial institution when the financial institution evaluates the information and informs the individual of the outcome of that evaluation.

In addition to being consistent with the language of the statute, the proposed definition of ''consumer'' is consistent with one of the primary purposes of Title V of G-L-B Act, namely, to enable an individual to limit the sharing of nonpublic personal information by a financial institution with a nonaffiliated third party. The information provided by a person to a financial institution before a customer relationship is established is likely to contain precisely the types of information that the statute is designed to protect. This information is no less deserving of protection simply because an application is denied or withdrawn. For these reasons, the Commission has retained the individual whose application is evaluated by a financial institution as an example of ''consumer'' in § 313.3(e)(2)(i).

Loan sales. Several commenters requested clarification of whether an individual becomes a consumer in various other scenarios involving loans. Commenters posited a wide variety of examples, which, if each were to be addressed specifically in the rule, would require a final rule of enormous complexity and detail. The Commission believes that a rule setting forth a general principle that is flexible enough to be applied in the array of loan transactions posited by the commenters is more appropriate. Towards this end, the Commission's rule provides, by example at § 313.3(e)(2)(iv), that a person will be a consumer of any entity that holds ownership or servicing rights to an individual's loan. [14] Financial institutions that own or service a loan are providing a financial product or service to the individual borrower in question. In some cases, the product or service is the funding of the loan, directly or indirectly. In other cases, the product or service is the processing of payments, sending account-related notices, responding to consumer questions and complaints about the handling of the account, and so on. The rule defines ''consumer'' in a way that covers individuals receiving financial products or services in each of these situations.

Agents of financial institutions. Several commenters agreed with the principle set out in the proposed rule that an individual should not be considered to be a consumer of an entity that is acting as agent for a financial institution. These commenters noted that the financial institution that hires the agent is responsible for that agent's conduct in carrying out the agency responsibili ties. The Commission agrees that the purposes of the G-L-B Act will be met provided the activities of the agent are the responsibility of the financial institution, and, therefore, the financial institution fulfills any obligations regarding the agent's handling of consumer information that otherwise would fall on the agents. [15] Of course, those providing services to a financial institution will also be subject to the limitations on reuse of information. *See* § 313.3(e)(2)(v).

Legal representative. The Commission also agrees with the suggestion made by several commenters that the definition of ''consumer'' should clarify that the obligations stemming from a consumer relationship may be satisfied by dealing either with the individual who obtains a financial product or service from a financial institution *or* that individual's representative. The Commission does not intend for the rule to require a financial institution to send opt out and initial notices to *both* the individual and the individual's legal representatives and has amended the final rule accordingly in § 313.3(e)(1).

Trusts. The Commission and the other Agencies received several comments concerning whether an individual who obtains financial services in connection with trusts is a consumer or customer of a financial institution. Several commenters urged the Agencies to exempt generally a financial institution from the requirements of the rule when it acts as a fiduciary, or, in the alternative, to clarify the categories of individuals that are considered to be customers. Commenters proposed, for example, that individuals who are beneficiaries with current interests should be identified as customers, whereas individuals who are only contingent beneficiaries should not be customers. Other commenters stated that when the financial institution serves as trustee of a trust, neither the grantor nor beneficiary is a consumer or customer under the rule. In these commenters' view, the trust itself is the institution's ''customer,'' and, therefore, the rule should not apply to a financial institution when it acts as trustee. These commenters also stated that when a financial institution is a trustee, it serves as a fiduciary and is subject to other obligations to protect the confidentiality of the beneficiaries' information that are more stringent than those under the provisions in the G-L-B Act. Similarly, these and other commenters claimed that an individual who is a participant in an employee benefit plan administered or advised by a financial institution does not qualify as a consumer or customer. The commenters opined that the plan sponsor, or the plan itself, is the ''customer'' for the purposes of the proposed rule. These commenters contended that plan participants have no direct relationship with the financial institution and, in any event, the financial institution is authorized to use information that would be covered under the G-L-B Act only in accordance with the directions of the plan sponsor. The commenters concluded, therefore, that the regulations should specifically exclude individuals who are participants in an employee benefit plan from the definition of consumer.

The definition of ''consumer'' in the G-L-B Act does not squarely resolve whether the beneficiary of a trust is a consumer of the financial institution that is the trustee. One consideration is that a financial institution that is a trustee assumes obligations as a fiduciary, including the duty to protect

[14] Such a person may not be a customer, however. *See* explanation of how the definition of ''customer'' will be applied in the loan context, in the discussion of the definition of § 313.3(h) and (i) below. *See also* § 313.4(c)(2) and (3)(ii) for further discussion concerning when a borrower establishes a customer relationship in the context of a loan sale.

[15] Of course, in some cases two institutions will each provide a financial service to the consumer as part of the same transaction, such as a loan broker that locates a creditor who makes a loan to the individual, in which case the consumer will have a customer relationship with both financial institutions.

the confidentiality of the beneficiaries' information, that are consistent with the purposes of the G-L-B Act and enforceable under state law. The Commission agrees with the commenters who concluded that, when the financial institution serves as trustee of a trust, neither the grantor nor the beneficiary is a consumer or customer under the rule. Instead, the trust itself is the institution's ''customer,'' and therefore, the rule does not apply because the trust is not an individual. Similarly, the Commission has excluded an individual who is a beneficiary of a trust or a plan participant of an employee benefit plan from the definitions of ''consumer'' and ''customer.'' Nevertheless, the Commission believes that an individual who selects a financial institution to be a custodian of securities or assets, for example in an IRA, is obtaining a financial product or service from the financial institution and is, therefore, a ''consumer'' under the G-L-B Act. The Commission has included examples in the rule that appropriately illustrate this interpretation of the G-L-B Act in §§ 313.3(e)(2)(vi)–(viii) and 313.3(i)(2)(i)(D).

Requirements arising from consumer relationship. While the proposed and final rule defines ''consumer'' broadly, this will not result in any additional burden to a financial institution in situations where (a) no customer relationship is established and (b) the institution does not intend to disclose nonpublic personal information about a consumer to nonaffiliated third parties. Under the final rule, a financial institution is under no obligation to provide a consumer who is not a customer with any privacy disclosures unless it intends to disclose the consumer's nonpublic personal information to nonaffiliated third parties outside the exceptions in §§ 313.14 and 313.15. A financial institution that wants to disclose a consumer's nonpublic personal information to nonaffiliated third parties is not prohibited by the rule from doing so, if the requisite notices are delivered and the consumer does not opt out. Thus, a financial institution that does not wish to be subject to the disclosure obligations of the rule as it applies to consumers who are not customers may simply decide not to share consumers' information with nonaffiliated third parties. Conversely, if a financial institution determines that the benefits of such sharing outweigh the attendant burdens, the financial institution is free to do so provided it notifies consumers about the disclosure and affords them a reasonable opportunity to opt out. In this way, the rule attempts to strike a balance between protecting an individual's nonpublic personal information and minimizing the burden on a financial institution.

f. *Consumer reporting agency.* The proposal adopted 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)). It is used in §§ 313.6(c), 313.12(a), and 313.15(a)(5) of the final rule.

The Commission received no comments suggesting any changes to this definition. Accordingly, the definition is adopted as proposed.

g. *Control.* The proposal defined ''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 § 313.3(a), above), and would result in financial institutions being considered as affiliates regardless of whether the control is by a company or individual.

The Commission received few comments in response to this definition. Some commenters suggested that a definition that did not require 25% ownership be adopted, while others suggested adopting a test focused solely on percent of stock owned in a company so as to avoid the uncertainties arising from a ''control in fact'' test.

The Commission believes that the proposed test is sufficiently well established and has concluded that an alternative test to be used solely in the privacy rule could create confusion. The Commission also believes that any test based only on stock ownership is unlikely to be flexible enough to address all situations in which companies are appropriately deemed to be affiliated and that including the stock ownership as one measurement of control provides necessary flexibility. Accordingly, the Commission adopts the definition of ''control'' as proposed.

h. *Customer.* The proposal defined ''customer'' as any consumer who has a ''customer relationship'' with a particular financial institution. As is explained more fully in the discussion of § 313.4, below, a consumer is a customer of a financial institution when the consumer has a continuing relationship with the institution.

The Commission received a large number of comments on the definition of ''customer'' and ''customer relationship.'' Given the interdependence of the two terms, the following analysis of the comments received will address both under the heading ''customer relationship.''

i. *Customer relationship.* The proposed rule defined ''customer relationship'' as a continuing relationship between a consumer and a financial institution whereby the institution provides a financial product or service that is to be used by the consumer primarily for personal, family, or household purposes. As noted in the proposal, a one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. A consumer would not become a customer simply by repeatedly engaging in isolated transactions that by themselves would be insufficient to establish a customer relationship, such as withdrawing funds at regular intervals from an ATM owned by an institution at which the consumer has no account. However, an individual who becomes the client of a loan brokerage, tax preparation firm, or financial counseling service would be a customer. The proposal also stated that a consumer would 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. The Commission received a large number of comments on this definition, as discussed below.

Point at which one becomes a customer. The Commission received many comments in response to the definitions of ''customer'' and ''customer relationship.'' Some commenters criticized what they considered to be the ill-defined line distinguishing consumers from customers. These commenters stated that the proposed distinction makes it difficult for a financial institution to know when the obligations attendant to a customer relationship arise. Several suggested that the distinction should be based on when a consumer and financial institution enter into a written contract for a financial product or service.

The Commission recognizes that the distinction between consumers and customers will, in some instances, require a financial institution to evaluate whether the particular facts of its consumer transactions fit within the definition of customer relationship. In those cases where an individual engages in a transaction that is isolated in nature (such as ATM transactions, purchases of money orders, or cashing of checks), the individual will not have established a customer relationship as a result of that transaction. In other situations, where a consumer typically would receive some measure of service such that the consumer's contact with the financial institution is more significant (such as would be the case when a consumer

borrows money, obtains investment advice, or becomes the client of an institution for the purpose of receiving tax preparation, loan brokerage, or credit counseling services), a customer relationship will be established. In those cases, the nature of the relationship indicates that it is not an isolated transaction, even though it may be short-term in duration.[16] The Commission believes that the distinction set out in the proposed rule, as further clarified by the examples in the final rule regarding the establishment of a customer relationship, provides sufficiently clear principles that can be applied to most fact situations that arise in the financial marketplace.

Customer relationship defined by written contract. The Commission agrees with those commenters who consider the execution of a written contract by a consumer and financial institution as clear evidence that a customer relationship has been established. The proposal cited the execution of a written contract as an example of when a customer relationship is established, and the final rule retains that example in § 313.4(c)(3)(i)(B). However, a test based solely on whether there is a written contract could inappropriately exclude situations in which an individual is a customer of a financial institution as a result of obtaining, for instance, financial, economic, or investment advisory services from a financial institution. Accordingly, the final rule does not define a customer relationship solely by the execution of a written contract.

Purchase of insurance. Other commenters suggested that, in the context of financial institutions that engage in the sale of insurance, the customer should be the policyholder and not the beneficiary. The Commission agrees and has retained the example in § 313.3(i)(2)(i)(C) of purchasing an insurance product as one situation in which a customer relationship is formed.[17] In this case, the person obtaining a financial product or service from the financial institution is the person purchasing the policy. The beneficiaries would be recipients of the insurance proceeds, thereby entitling them to the protections afforded consumers.

Sales of loans. As previously noted, several commenters raised questions in the context of loan sales. Many commenters stated that, under the final rule, a person should not be considered a customer of two financial institutions when the originating bank sells the servicing rights. A point consistently made by these commenters was that a borrower would be equally well protected with less risk of confusion if the borrower is deemed to be a customer of only one entity in connection with a loan, with that entity perhaps being the party with whom the borrower communicates about the loan. The Commission believes that it is appropriate to consider a loan transaction as giving rise to only one customer relationship, with the recognition that this customer relationship may be transferred in connection with a sale of part or all of the loan. In this way, the borrower will not be inundated by privacy notices (but rather will normally receive annual notices from the loan servicer), many of which might be from subservicers that the borrower did not know had any connection to his or her loan. However, that customer will remain a consumer of the entity that transfers the servicing rights, as well as a consumer of any other entity that holds an interest in the loan.

In order to satisfy the statutory requirement that a customer receive an annual notice from a financial institution until that relationship terminates, the final rule provides that the borrower must be deemed to have a customer relationship with at least one of the entities that hold an interest in the loan. A financial institution that makes a loan, retains it in its portfolio, and provides servicing for the loan clearly would have a customer relationship with the borrower. More complex, however, are situations in which servicing is sold or investors purchase a partial interest in a loan. The Commission has adopted an approach designed to ensure that a customer receives annual notices for the duration of the customer relationship from the most appropriate financial institution.

Under the final rule, as stated in § 313.3(i)(2)(i)(B), a customer relationship will be established as a general rule with the financial institution that makes a loan to an individual. This customer relationship then will attach to the entity providing servicing. Thus, if the originating lender retains the servicing, it will continue to have a customer relationship with the borrower and will be obligated to provide annual notices for the duration of the customer relationship. If the servicing is sold, then the purchaser of the servicing rights will establish a customer relationship (and the originating lender will have a consumer relationship with the borrower). *See* § 313.3(i)(2)(ii)(B). In this way, the borrower will be entitled to receive an initial notice and annual notices from the loan servicer, but will not be inundated by initial and annual notices from entities that hold interests in the loan but are unknown to the consumer (and who do not share the consumer's nonpublic personal information with unaffiliated third parties).

Collection agencies that purchase accounts in their own name. The Commission received a substantial number of comments from different types of debt collectors and their representatives. This section addresses several comments the Commission received concerning the proposed rule's differentiation between collectors who assist creditors in collecting delinquent accounts, and those who purchase them in their own name.[18] The Commission also received comments from all types of collection agencies on other points. Several contested the Commission's treatment of debt collectors as financial institutions.[19] Others were concerned that the rule would prohibit communications with a creditor that retained ownership on the account and hired the agency to obtain payment from debtors.[20]

Representatives of two major trade associations of debt collectors pointed to the definitions set forth in section 803 of the Fair Debt Collection Practices Act, which specifically exempts any ''creditor'' collecting its own accounts in its own name from being within the definition of a ''debt collector'' subject to that statute, and the case law holding that the ''creditor'' exemption does not include debt collectors that purchase defaulted accounts in their own name

[16] Many of the customer relationships established by institutions under the Commission's jurisdiction may well be short-term, as can be seen from the examples in § 313.5(b)(2) of when a customer relationship terminates.

[17] Despite its lack of enforcement jurisdiction over persons providing insurance, the Commission retains this example because it may be useful in evaluating analogous situations. Some commenters also asked for further clarification of ''purchase'' in this context. The Commission does not believe such clarification is necessary and has retained the example as proposed.

[18] ''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.'' 65 FR 11174 at 11176 (Mar. 1, 2000).

[19] Those issues are discussed under §§ 313.1(b), 313.3(k) and 313.4.

[20] This fear is unfounded, because such a communication by a collection agency reporting to a creditor that has retained ownership of an account would be permitted under § 313.15(a)(2)(iv). That section allows communications to parties holding a legal interest relating to the consumer, which would certainly include a creditor that owns the debt.

for collection.[21] The commenters argued that, because the FDCPA does not treat collection agencies that purchase defaulted accounts in their own name as creditors, the G-L-B Act should not be interpreted to do so. In addition, debt buyers stated that they frequently made bulk purchases of defaulted accounts from creditors, immediately discarded and never even attempted to collect many of the accounts they purchased, and were unable to locate many of the account debtors from whom they wanted to collect amounts due.

The Commission recognizes that these businesses have some attributes of creditors who buy active accounts (where the debtors clearly become customers of the account purchaser) and some attributes of regular debt collectors who attempt to collect amounts due on behalf of the creditor (where the debtors clearly remain the creditor's customer). After careful consideration of the comments and the purposes of the Act, the Commission retains its view that if a business purchases a defaulted account for collection, it may establish a ''customer relationship'' with the account debtor. However, such a relationship occurs only in those instances where the agency locates the individual and tries to obtain payments on the debt. This approach reflects the reality that the collector has purchased the account (albeit for less than it would pay for a current account) and avoids the result that otherwise the individual would not have a ''customer relationship'' with anyone because the former relationship with the creditor will have been terminated. At the same time, it responds to industry commenters that contested the Commission's previous position that purchase of the account automatically establishes a customer relationship. The applicable example in § 313.3(i)(2)(i)(J) makes it clear that a debt buyer does not have a customer relationship if it does not attempt to collect payments from, or is unable to locate, the individual named on an account it has purchased.

Brokers. Several commenters suggested that the use of a mortgage broker, or other business that procures credit on behalf of a consumer, such as financing to purchase an automobile, should not create a customer relationship. The Commission disagrees. A relationship between such a business and a consumer is more than an isolated transaction, given that the broker will likely provide significant services for a consumer, such as providing information or advice about financing options, actively assisting the consumer in contacting potential financing sources, analyzing financial information, or performing credit checks. In some cases, the broker will also negotiate with other financial institutions on the consumer's behalf and/or assist with paperwork and loan closings. In light of the nature of the services provided by a loan broker or other credit arranger in assisting the consumer with financial transactions, it is appropriate to consider the business to be a financial institution that establishes a customer relationship when it undertakes to arrange or broker a home mortgage loan or other credit for the consumer. The final rule reflects this conclusion in § 313.3(i)(2)(i)(E).

IRA Custodians. The final rule adds an example in § 313.3(i)(2)(i)(D) to clarify that an individual will be deemed to establish a customer relationship when a financial institution acts as a custodian for securities or assets in an IRA. This example is consistent with the explanation set out above in the discussion of ''consumer'' concerning trusts.

j. *Federal functional regulator.* The proposal sought comment on a definition of ''government regulator'' that included all of the Agencies and State insurance authorities under the circumstances identified in the definition.[22]

The few comments that were received on this definition suggested that it be expanded to include additional governmental entities. The Commission notes that, for purposes of the privacy rule, this term (which does not include the Commission) is relevant only in the discussion of when a financial institution may disclose information to a law enforcement agency. The exception as stated in the statute uses the term ''federal functional regulator'' (*see* section 502(e)(5)), which term is defined in the statute at section 509(2) and also includes the Commission and Secretary of the Treasury, for purposes of the exception permitting disclosures to law enforcement agencies. The Commission has decided simply to use the statutory term.

k. *Financial institution.* The Commission's proposed rule defined financial institution as ''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 * * *'' Through the examples, the Commission expressed its view that an institution is a financial institution ''the business of which is engaging in activities that are financial in nature'' only if the entity is significantly engaged in such activities. The Commission received numerous comments concerning this definition.

Some commenters requested that the Commission adopt the definition of financial institution contained in the other Agencies' definition. The other Agencies defined financial institution as ''any institution the business of which is engaging in activities that are financial in nature *or incidental to such financial activities* as described in section 4(k) of the Bank Holding Company Act.'' Section 509(3) of the G–L–B Act defines the term as ''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.'' Section 4(k) of the Bank Holding Company Act refers to three types of activities that the Board may determine permissible for financial holding companies: those that are financial in nature, those that are incidental to such financial activity, and those that are complementary to financial activities. The Commission interprets the G-L-B Act to refer to those activities in Section 4(k) that are described as financial in nature at present, and not to include automatically those activities that the Board later determines are incidental or complementary to financial activities. Such activities are not necessarily themselves financial activities and, therefore, should not have an impact on the definition of financial institution. Thus, the final rule incorporates the statutory language in § 313.3(k).[23]

Given the breadth of the definition, some commenters requested that the Commission provide a definitive list of the entities that are subject to the rule. The Commission deems it inappropriate to publish such a definitive list. The institutions covered by the rule currently are defined by reference to the comprehensive list of activities found at section 4(k)(4) of the Bank Holding Company Act.[24] The Commission has

[21] 15 U.S.C. 1692a(4) and 1692a(6). *Cirkot v. Diversified Fin. Sys., Inc.,* 839 F. Supp. 941, 944–45 (D. Conn. 1993); *Holmes v. Telecredit Service Corp.,* 736 F. Supp. 1289, 1293 (D. Del. 1990); *Kimber v. Federal Fin. Corp.,* 668 F. Supp. 1480, 1485–86 (D. Ala. 1987).

[22] This term was used in the exception set out in § 313.11(a)(4) of the proposal as it related to disclosures to law enforcement agencies, ''including government regulators.''

[23] *See also* the discussion of the effective date at § 313.18, *infra.* Section 4(k) of the Bank Holding Company Act established procedures whereby the Board can add activities to the list of activities that it is permissible for financial holding companies to engage in. To the extent these later added activities are financial activities, and not incidental activities, the rule will not be effective as to those new financial institutions until the Commission so determines.

[24] See footnotes 5–8 and accompanying text, *supra.* These are activities either specified in

reformatted and added additional examples of financial institutions in the final rule to guide the analysis of whether a particular entity is a financial institution through reference to section 4(k)(4) and particular sections of the Board regulations that are incorporated therein by reference.

The Commission received several comments on the ''significantly engaged'' standard set forth in the examples in the proposed rule. A few expressed concern that the ''significantly engaged'' test was too imprecise to allow some businesses to know whether they were within the definition, usually suggesting alternatives that would exclude the industries they represent. The final rule does not define ''significantly engaged.'' The revenue tests suggested by some commenters are too inflexible to take into consideration all instances where an institution may be significantly engaged in a financial activity. The final rule retains the flexibility of the ''significantly engaged'' standard and provides guidance through examples. To that end, the Commission has moved the ''significantly engaged'' language into the text of the final rule and retains in the final rule those examples from the proposed rule of entities that are and are not significantly engaged in a financial activity. A retail business that issues its own credit card directly to consumers is a financial institution significantly engaged in the extension of credit, but a retail business that merely allows its retail clients to make payments through occasional lay-away plans is not significantly engaged in a financial activity. Similarly, a small merchant that informally extends credit when it ''runs a tab'' for some individuals is not significantly engaged in the business of extending credit. The Commission believes that the concept of ''significantly engaged'' is sufficiently clear to provide guidance to most entities in analyzing their specific factual situations.

Many commenters, especially some representatives of the consumer debt collection industry,[25] expressed concern at the breadth of the definition and asserted that Congress could not have intended to include all institutions that engage in the activities referenced in Section 4(k). The plain language of the statute, however, dictates that breadth and grants the Commission no authority to exclude particular entities from the definition. The broad scope of the Act, and the comments received by the Commission, are also discussed above in more detail in the context of § 313.1(b). While it is not possible to discuss every potential financial institution in detail, the Commission specifically sought comment on certain of the activities listed in section 4(k) and the Board regulations that are incorporated by reference.

The proposed rule acknowledged that one of the activities characterized as financial in nature in Section 4(k)(4) of the Bank Holding Company Act is operating a travel agency in connection with offering financial services.[26] The Commission received few comments on the extent to which travel agents operate in connection with financial services. The comments did indicate that travel agents generally do sell travelers checks, trip insurance, and travel insurance, all of which constitute financial products or services. However, the Commission does not consider a travel agency's operations to be ''in connection with offering financial services'' and therefore covered simply because it offers travelers checks or travel related insurance to their travel clients. Rather, the Commission interprets the G-L-B Act to cover travel agencies only if their travel-related services are offered in addition to offering other financial services.[27] This would cover, for example, entities that offer credit, investment, or insurance products or services, and also offer travel-related services to their clients. For these types of entities, travel operations would thereby become covered services and their travel transactions would be protected by the G-L-B Act.[28]

Some commenters requested clarification concerning whether certain Internet industries are affected by the rule. The comments in this regard did not provide sufficient detail for the Commission to evaluate all of the concerns of the commenters, but the Commission notes that institutions operating on-line, like those operating off-line, will have to evaluate (1) whether they are engaged in a financial activity, and (2) if so, whether they have consumers or customers that trigger the disclosure or other requirements of the Act. On a related issue, the Commission notes that one of the financial activities incorporated by reference into Section 4(k) of the Bank Holding Company Act is:

> ''providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if * * * [t]he data to be processed or furnished are financial, banking, or economic * * *.''

12 CFR 225.28 (b)(14). The Commission notes with respect to this activity that financial software and hardware manufacturers, as described, are financial institutions but will have no disclosure obligations if they sell only to businesses. Furthermore, in the case of an isolated one-time sale of software or hardware to a consumer, their disclosure obligations would be very limited. In addition, this language brings into the definition of financial institution an Internet company that compiles, or aggregates, an individual's on-line accounts (such as credit cards, mortgages, and loans) at that company's web site as a service to the individual, who then may access all of its account information through that Internet site.

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.'' Several commenters supported this distinction and the Commission retains it here. For example, management consulting is a ''financial activity'' but it is not likely

Section 4(k)(4) itself, or are activities listed in Board regulations referenced in Section 4(k)(4) already in effect on the effective date of the G–L–B Act. This list of activities may expand as the Board exercises its authority to add additional activities that are financial in nature pursuant to Section 4(k)(1–3) of the Bank Holding Company Act.

[25] The statute is clear that debt collection agencies are financial institutions under its terms. As noted in the discussion of the definition of ''financial institution'' below, the statute treats a broad range of activities as ''financial in nature.'' Section 509(3) of the G-L-B Act 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.'' Section 4(k)(4)(F) of the Bank Holding Company Act includes all financial activities deemed by the Federal Reserve Board ''to be so closely related to banking or managing or controlling banks as to be a proper incident thereto.'' In Regulation Y, 12 CFR 225.28(b)(2)(iv), the Board specifically designated ''collection agency services'' as such a financial activity.

[26] *See* footnote 5 of the Commission's discussion of the proposal at 65 FR 11176. Section 4(k)(4)(G) of the Bank Holding Company Act includes all financial activities conducted in the United States deemed by the Federal Reserve Board ''to be usual in connection with the transaction of banking or other financial operations abroad.'' In Regulation K, 12 CFR 211.(d)(15), the Board specifically designated ''[o]perating a travel agency * * * in connection with financial services'' as such a financial activity.

[27] This analysis is consistent with an interim rule published by the Board at 12 CFR 225.86(b)(2), in which it characterized the travel agency activity ''operating a travel agency in connection with financial services offered by the financial holding company or others.'' 65 FR 14433, 14439 (Mar. 17, 2000).

[28] *See* the Commission's discussion of ''financial product or service'' in the next section, as it relates to the Act's inapplicability to nonfinancial products or services of financial institutions.

that any individual obtains management consulting services for personal, family or household purposes. Likewise, courier services, data processors, and real estate appraisers 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.[29] The Commission declines to adopt a definitive list, as requested by some commenters, of all of the financial institutions that do not have consumers and customers. Such a list inevitably will not be exclusive and may include some institutions that operate so that in some instances they have consumers and customers and in others they do not.

Some commenters suggested that sole proprietors be exempt from the definition, but provided no helpful rationale for doing so, while others requested clarification as to whether nonprofit entities could be financial institutions covered by the rule. Whether or not a commercial enterprise is operated by a single individual is not determinative in analyzing whether the entity is a ''financial institution.'' If an individual is in the ''business of * * * engaging in financial activities * * *,'' that ''business'' is included within the ''financial institution'' definition.[30] Similarly, nothing in the definition of financial institution excludes nonprofit entities from the definition of financial institution.

Few commenters addressed proposed § 313.3(j)(3)(iii), which incorporated the Act's exemption 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 nonaffiliated third party. This exemption applies 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 (§§ 313.14 and 313.15 in the final rule). The Commission also sought comment on whether it should require chartered institutions, as a condition of their exemption, to enter into a confidentiality agreement with any nonaffiliated third parties with whom they share information pursuant to the exceptions. Chartered institutions supported the interpretation; one commenter contended that such additional language was not in keeping with the intent of the exemption. The Commission believes that its interpretation merely operates to allow chartered institutions to continue their normal business, and does not permit them (or any party receiving information from them) to disclose information unrestrained. In accord with the limitations on reuse and redisclosure in section 502(c) of the G–L–B Act, both chartered institutions and recipients of nonpublic personal information are limited in that regard. The Commission has adopted the provision as proposed.

l. *Financial product or service.* The proposal defined ''financial product or service'' as a product or service that a financial institution could offer by engaging in an activity that is financial in nature under section 4(k) of the Bank Holding Company Act of 1956. The proposal's definition included 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 included the brokerage and distribution of information about a consumer for the purpose of assisting the consumer in obtaining a financial product or service.

The most frequent comment on this proposed definition was that the evaluation of application information should not be considered a financial product or service. For the reasons advanced above in the discussion of the definition of ''consumer,'' the Commission concludes that it is appropriate to retain evaluation activity within the scope of financial product or service covered by the rule. Evaluation is one of many financial services provided by financial institutions. Moreover, a consumer is likely to provide the type of information that the statute is designed to protect in the course of obtaining the financial institution's evaluation.

An entity's status as a financial institution does not cause every product or service offered by that entity to be a financial product or service. A retailer that issues its own credit card directly to consumers provides a financial service (credit) to consumers who utilize the card; but when that same retailer sells merchandise, it provides a nonfinancial product or service (retail sale of merchandise).

The Commission has retained the essence of the proposed definition, but has revised § 313.(l)(1) to mirror its change to the definition of ''financial institution'' in § 313.3(k) and eliminated the word ''distribution'' from § 313.3(l)(2) because it is not intended to mean anything different from ''brokerage'' and, therefore, its use invites confusion.

m. *Nonaffiliated third party.* The proposal defined ''nonaffiliated third party'' as any person (which includes natural persons as well as corporate entities) except (1) an affiliate of a financial institution and (2) a joint employee of a financial institution and a third party. The proposal clarified the circumstances under which a company that is controlled by a financial institution pursuant to that institution's merchant banking activities or insurance company activities would be a ''nonaffiliated third party'' of that financial institution.

The Commission received very few comments in response to this proposed definition. One commenter requested that the final rule provide that a disclosure of information to someone who is serving as a joint employee of two financial institutions should be deemed to have been disclosed to both financial institutions. The Commission disagrees with this result. Instead, the Commission believes it is appropriate to deem the information to have been given to the financial institution that is providing the financial product or service in question. Thus, if an employee of a mortgage lender is a dual employee with a securities firm, information received by that person in connection with a securities transaction conducted with the securities firm would be deemed to have been received by the securities firm.

The Commission notes that its proposal omitted a section included in the other Agencies' rules relating to companies engaged in merchant banking, investment banking, or investment activities described in section 4(k)(4)(H–I) of the Bank Holding Company Act. For purposes of consistency with the rules to be adopted by the other Agencies, the Commission has included it at § 313.3(m)(2). Otherwise, the final rule defines ''nonaffiliated third party'' as proposed.

n. *Nonpublic personal information.* Section 509(4) of the G-L-B Act defines ''nonpublic personal information'' to mean ''personally identifiable financial information'' that is provided by a consumer to a financial institution, results from any transaction with the

[29] If such financial institutions receive consumers' nonpublic personal information from nonaffiliated financial institutions pursuant to one of the exceptions set forth in §§ 313.14 and 313.15, however, they would be required to observe the § 313.11 limitations on reuse and redisclosure of that information.

[30] An individual who provides a financial service only informally (*e.g.,* preparing tax forms without remuneration for friends or family, or as community service) is not likely significantly engaged in a financial activity.

consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. It also includes any ''list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information.'' The statute excludes publicly available information (unless provided as part of the list, description or other grouping described above), as well as a list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using nonpublic personal information. The statute does not define either ''personally identifiable financial information'' or ''publicly available information.''

The proposed rule restated the categories of information described above and presented two alternative approaches to identifying what information would be regarded as publicly available (and therefore, as a general rule, outside the definition of ''nonpublic personal information''). Alternative A deemed information as publicly available only if a financial institution *actually obtained* the information from a public source while Alternative B treated information as publicly available if a financial institution *could* obtain it from such a source. Both Alternatives A and B included within the definition of ''nonpublic personal information'' publicly available information that is provided as part of a list, description, or other grouping of consumers. In addition to requesting comment on Alternatives A and B, the Commission requested comment concerning whether a variation of the two alternatives should be adopted that would require a financial institution to undertake reasonable procedures to establish that information is, in fact, publicly available.

Commenters favoring Alternative A noted that it provided the greatest protection for consumers by treating anything the consumer gives to a financial institution to obtain a financial product or service as nonpublic personal information. Under Alternative A, this protection would be lost only if a financial institution actually obtained the information from a public source. These commenters also preferred the bright-line distinction drawn by treating as nonpublic personal information any information given by a consumer to obtain a financial product or service or information that results from transactions between a financial institution and a consumer. However, the majority of those commenting on this issue favored Alternative B, noting that this alternative was consistent with the statute and would be far less burdensome on financial institutions. These commenters suggested that a requirement that the information actually be obtained from a public source would impose needless burdens on financial institutions (by requiring, for instance, that a financial institution ''tag'' information they obtained from public records) and is not required by the statute.

The final rule incorporates the benefits of both alternatives. Under the final rule, information will be deemed to be ''publicly available'' and therefore excluded from the definition of ''nonpublic personal information'' if a financial institution has a reasonable basis to believe that the information is lawfully made available to the general public from one of the three categories of sources listed in the rule. *See* § 313.3(p)(1). The final rule provides that a financial institution will have a ''reasonable basis'' for believing that information is lawfully made available if the financial institution has taken steps to determine whether the information is of the type that is available to the general public, whether an individual can direct that the information not be made available to the general public, and, if so, that the financial institution's particular consumer has not so directed. In this way, a financial institution will be able to avoid the burden of having to actually obtain information from a public source, but will not be free simply to assume that information is publicly available without some reasonable basis for that belief.

An example of information a financial institution might have a reasonable basis to believe is publicly available, cited in the final rule, is the fact that someone has a loan that is secured by a mortgage, as long as the financial institution has determined that the mortgage information is included on the public record in the relevant jurisdiction. *See* § 313.3(p)(3)(iii)(1). The rule also explains that a financial institution will have a reasonable basis to believe that a telephone number is publicly available only if the institution has either located the number in a telephone book or has been informed by the consumer that the number is not an unlisted telephone number. *See* § 313.3(p)(3)(iii)(2). This approach is based on the underlying principle that a financial institution should not automatically assume that an individual's information is publicly available, especially if a consumer has some measure of control over the public availability of the information.

With regard to some types of information that may be available to the general public, the extent to which a consumer can control the release of that information should be well known. For example, in most jurisdictions, a borrower has no choice about whether a lender will make a mortgage a matter of public record; a lender must do so in order to protect its security interest. In the case of a telephone number, it is well established that a person may request that his or her number be unlisted; thus, the financial institution will have to takes steps to determine whether a particular consumer has exercised that option. In other instances, there will be more variation on the general availability of the information and the consumer's right to direct that it not be disclosed. Some jurisdictions, for example, make driver's license information more available than others.[31] In evaluating whether it is reasonable to believe that information is publicly available, a financial institution must consider whether the information is of a type that a consumer could keep from being a matter of public record.

To implement the Act's complex definition of ''nonpublic personal information'' that is provided in the statute, the final rule adopts a definition that consists, generally speaking, of (1) personally identifiable financial information, plus (2) a consumer list (and publicly available information pertaining to the consumers on that list) that is derived using personally identifiable financial information that is *not* publicly available. From that body of information, the final rule excludes publicly available information (except as noted above) and any consumer list that is derived without using personally identifiable financial information that is not publicly available. *See* § 313.3(n)(1) and (2). Examples are provided in § 313.3(n)(3) to illustrate how this definition applies in the context of consumer lists.

o. *Personally identifiable financial information.* The proposed rule defined ''personally identifiable financial information'' to include information that a consumer provides to a financial institution in order to obtain a financial product or service, information resulting from any transaction between the consumer and the financial institution involving a financial product or service,

[31] The Driver's Privacy Protection Act, 18 U.S.C. 2721–2725, restricts the states' ability to disclose a driver's personal information without the driver's consent. *Reno* v. *Condon* __ U.S. __, 120 S. Ct. 666 (2000).

and information about a consumer a financial institution otherwise obtains in connection with providing a financial product or service to the consumer. The proposed rule also treated the fact that someone is a customer of a financial institution as personally identifiable financial information. In essence, the proposed rule treated any personally identifiable information as financial if it was obtained by a financial institution in connection with providing a financial product or service to a consumer. The Commission noted in the preamble to the proposed rule that this interpretation may result in certain information being covered by the rule that may not be considered intrinsically financial, such as health status.

The Commission received a large number of comments in response to this definition, most of which stated that the definition inappropriately included certain identifying information that is not financial, such as name, address, and telephone number. Many others maintained that ''personally identifiable financial information'' should not include the fact that someone is a customer of a financial institution. These commenters typically noted that many customer relationships are matters of public record (such as would be the case, for instance, anytime a transaction results in the recordation of a security interest) while other customer relationships are matters of public knowledge (because consumers frequently disclose the relationships by writing checks, using credit cards, and so on). Many commenters stated that aggregate data about a financial institution's customers that lack personal identifiers should not be considered personally identifiable financial information.

Treatment of identifying information as financial. The Commission continues to believe that any information should be considered financial information if it is requested by a financial institution for the purpose of providing a financial product or service. This approach is consistent with the broad definition of ''financial institution'' used in the statute, which encompasses not only traditional financial activities (such as banks, mortgage lenders, finance companies), but also a large number of entities that engage in activities not traditionally considered financial (such as financial career counselors, insurance companies, and data processors). As a consequence of that definition, the range of information that has a bearing on the terms and availability of a financial product or service or that is used by a financial institution in connection with providing a financial product or service is extremely broad and may include, for instance, medical information and other sorts of information that might not be thought of as financial.

Many commenters, including several hundred private investigators, expressed concern about the need for ready access to identifying information to locate people attempting to evade their financial obligations. These commenters consistently suggested that names, addresses, and telephone numbers should not be treated as financial information. However, financial institutions rely on a broad range of information that they obtain about consumers, including information such as addresses and telephone numbers, when providing financial products or services. Location information is used by financial institutions to provide a wide variety of financial services, from the sending of checking account statements to the disbursing of funds to a consumer. Other information, such as the maiden name of a consumer's mother often will be used by a financial institution to verify the consumer's identity. The Commission concluded that it would be inappropriate to carve out certain items of information that a particular financial institution might rely on when providing a particular financial product or service.

The Commission notes that names, addresses, and telephone numbers, if publicly available, will not be subject to the opt out provisions of the statute unless that information is ''derivative information'' (*i.e.,* information that is part of a list, description, or other grouping of consumers that is derived from personally identifiable financial information that is not publicly available). Thus, in instances involving specific requests about individuals, a financial institution still may disclose information about the individual that the institution has a reasonable basis to believe is publicly available, provided that in so doing the institution does not disclose the existence of a customer relationship (unless the relationship is a matter of public record, as in the case of most mortgage loans). Moreover, in instances when a consumer does not opt out, a financial institution may disclose any nonpublic personal information to a nonaffiliated third party provided that the disclosure is consistent with the institution's opt out and privacy notices.

Customer relationship as ''personally identifiable financial information.'' The Commission disagrees with those commenters who maintain that customer relationships should not be considered to be personally identifiable financial information. Information that a particular person has a customer relationship identifies that person, and thus is personally identifiable. This information also is financial, because it communicates that the person in question has a transaction involving a financial product or service with a financial institution. While this information could in certain cases be a matter of public record, that does not change the analysis of whether the information is personally identifiable financial information.

Changes made to the definition. The final rule makes various stylistic changes to the definition to make it easier to read and understand. In addition, the final rule adds to the examples of information covered by the rule any information that the institution collects through a ''cookie.'' [32] *See* § 313.3(o)(2)(F). This illustrates one of the various means by which a financial institution may ''otherwise obtain'' information about a consumer in connection with providing a financial product or service to that consumer.

An example in § 313.3(o)(2)(ii)(B) clarifies that aggregate information or blind data lacking personal identifiers is not covered by the definition of ''personally identifiable financial information.'' The Commission agrees with those commenters who opined that such data, by definition, do not identify any individual.

p. *Publicly available information.* The proposal defined ''publicly available information'' to include information that is lawfully made available to the public from official public records (such as real estate recordations or security interest filings), 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 stated that publicly available information from widely distributed media would include information from an Internet site that is available to the general public without requiring a password or similar restriction.

As noted in the discussion of ''nonpublic personal information,'' the Commission proposed two versions of the definition of ''publicly available information.'' The final rule more closely tracks the statute while

[32] A cookie is a small text file placed on a consumer's computer hard drive by a web server. The cookie transmits information back to the server that placed it.

incorporating the benefits of both alternatives.

Several commenters questioned the appropriateness of excluding information from the definition of ''publicly available information'' if a person who seeks to obtain the information over the Internet must have a password or comply with a similar restriction. These commenters made the point that many Internet sites are available to a large number of people, each of whom need a user name and identification number to access the sites. Several of these commenters suggested that it is more appropriate to focus on whether the information was lawfully placed on the Internet.

The Commission agrees and has amended the final rule to remove the reference to passwords or similar restrictions from the example of the Internet as a ''widely distributed'' medium of communication. In its place, the Commission has substituted a standard requiring that the information be available on an unrestricted basis, and has then specified that a site is not restricted merely because an Internet service provider or a site operator requires a fee or password as long as access is otherwise available to the general public. The traditional use of passwords is to confine the access of individual customers to specific, individual information. However, website operators, in particular, may require user identifications and passwords as a method of tracking access rather than restricting access to the information available through the website. Fees may be levied to enhance the revenue of the Internet service provider or site operator rather than restrict access. Therefore, the Commission believes that the definition of ''widely distributed media'' should properly focus on whether the information is lawfully available to the general public, rather than on the type of medium from which information is obtained.

The concept of information being lawfully obtained was included in the proposal, and is retained in the final rule. Thus, information unlawfully obtained will not be deemed to be publicly available notwithstanding that it may be available to the general public through widely distributed media.

The following example illustrates how ''nonpublic personal information,'' ''personally identifiable financial information,'' and ''publicly available information'' will work under the final rule. Assume that Mary provides a mortgage lender with information in order to obtain a loan to finance a home purchase, and the same information to a retail store to open a credit card account. Under the final rule, all of this information would be personally identifiable financial information. Once Mary establishes the customer relationships she seeks, the fact that Mary is a mortgage loan customer and a credit card customer at the financial institutions also would be personally identifiable financial information.

Certain information provided by Mary, such as her name and address, may be publicly available. If the mortgage lender has a reasonable basis to believe that this information is publicly available, and if the information was included on a list of all of the institution's mortgage loan customers, then her name and address would fall outside the definition of ''nonpublic personal information'' in those jurisdictions where mortgages are a matter of public record. However, Mary's name and address would be protected as nonpublic personal information if the retailer wanted to include those items on a list of holders of its proprietary credit card. The difference in treatment stems from the distinction drawn in the statute between lists prepared using publicly available information (as would be the case in the mortgage loan hypothetical) and lists prepared using information that is not publicly available (as would be the case in the credit card hypothetical).

The Commission concludes that this relatively complex approach is mandated by the statute's definition of ''nonpublic personal information.'' The final rule also is consistent with the fact that certain relationships are matters of public record, and, therefore, less deserving of protection from disclosure.

q. *You.* The Commission used the pronoun ''you'' to refer to financial institutions within its jurisdiction in the proposal and defined ''you'' to mean those entities.

The Commission received no comments in response to this definition and adopts the definition set forth in the proposed rule.

Section 313.4 Initial Privacy Notice to Consumers 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 are not customers, the notice must be provided prior to disclosing nonpublic personal information about the consumer to a nonaffiliated third party.

The proposed rule implemented these requirements by mandating that a financial institution provide the initial notice to an individual prior to the time a customer relationship is established and the opt out notice prior to disclosing nonpublic personal information to nonaffiliated third parties. These notices were required to be clear and conspicuous and to accurately reflect the institution's privacy policies and practices. The proposal also set out standards governing when a customer relationship is established and how a financial institution is to provide notice.

The Commission received many comments on proposed § 313.4. Most of the comments raised questions about the time by which initial notices must be provided, whether new notices are required for each new financial product or service obtained by a customer, the point at which a customer relationship is established, and how initial notices may be provided.

Providing initial notices ''prior to'' time customer relationship is established. Many commenters stated that, because the statute requires only that the initial notice be provided ''at the time of establishing a customer relationship,'' the regulation should not require that the notice be provided ''prior to'' the point at which a customer relationship is established. These commenters were concerned that the rule could be interpreted as requiring a financial institution to provide disclosures at a point different from when they must provide other federally mandated consumer disclosures during the process of establishing a customer relationship.

In response to these comments, the Commission has clarified the timing for providing initial notices. The final rule provides that, as a general rule, the initial notice must be given not later than the time when a financial institution establishes a customer relationship. *See* § 313.4(a)(1). As in the proposal, the initial 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 TILA. This approach, like the approach taken in the proposed rule, strikes 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 otherwise result if the final rule were to require financial institutions to provide consumers with a series of notices at different times in a transaction.

Providing notices after customer relationship is established. Several commenters stated that the rule should provide financial institutions with the flexibility to deliver the initial notice after the customer relationship is established under certain circumstances. These commenters posited several situations in which a customer relationship is established without face-to-face contact between the consumer and financial institution. For example, collection agencies that purchase accounts in default noted that it frequently takes time to locate debtors on such accounts (and that sometimes they do not even try to do so.) The commenters stated that delivery of the initial notice *before* the customer relationship is established in these situations would be impractical, and a requirement along those lines would have a significant adverse effect on the ability to provide a financial product or service to a consumer as quickly as the consumer desires.

The Commission believes that it is appropriate for financial institutions to have flexibility in certain circumstances to provide the initial notice at a point after the customer relationship is established. To accommodate the wider range of situations presented by the commenters, the Commission has modified the relevant examples so that they now are more broadly applicable. As stated in the final rule in § 313.4(e), a financial institution may provide the initial notice within a reasonable time after establishing a customer relationship in two instances. First, notice may be provided after the fact if the establishment of the customer relationship is not at the customer's election. *See* § 313.4(e)(1)(i). This might occur, for instance, when a credit account is sold. Second, a notice may be sent after establishing a customer relationship when to do otherwise would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time. *See* § 313.4(e)(1)(ii). An example of this would be when a transaction is conducted over the telephone and the customer desires prompt delivery of the item purchased. Another example of when this might occur is when a lender (other than a college or university) establishes a customer relationship with an individual under a student loan program as described in the final rule where loan proceeds are disbursed promptly without prior communication between the bank and the customer.

In most situations, and particularly where the establishment of a customer relationship is in person, a financial institution should give the initial notice at a point when the consumer still has a meaningful choice about whether to enter into the customer relationship. The exceptions listed in the examples, while not exhaustive, illustrate the less frequent situations when delivery either would pose a significant impediment to the conduct of a routine business practice or the consumer agrees to receive the notice later in order to obtain a financial product or service immediately.

In circumstances when it is appropriate to deliver an initial notice after the customer relationship is established, a financial institution should deliver the notice within a reasonable time thereafter. For example, a debt buyer that has purchased a defaulted account for collection in its own name would be authorized by § 313.4(e)(2)(i) to provide its privacy notice shortly after locating the debtor. Several commenters requested that the final rule specify precisely how many days a financial institution has in which to deliver the notice under these circumstances. However, the Commission believes that a rule prescribing the maximum number of days would be inappropriate because (a) the circumstances of when an after-the-fact notice is appropriate are likely to vary significantly, and (b) a rule that attempts to accommodate every circumstance is likely to provide more time than is appropriate in many instances. Thus, rather than establish an inflexible rule, the Commission has elected to retain the more general rule as set out in the proposal in § 313.4(e)(1).

Nothing in the 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 individual to compare its privacy policies and practices with those of other institutions in advance of conducting transactions.

New notices not required for each new financial product or service. Several commenters asked whether a new initial notice is required every time a customer obtains a financial product or service from that financial institution. These commenters suggested that the public would not materially benefit from repeated disclosures of the same information, and that requiring additional initial notices to be provided to the same consumer would be burdensome on financial institutions.

The Commission agrees that it would be burdensome, with little corresponding benefit to the public, to require a financial institution to provide the same consumer with additional copies of its initial notice every time the consumer obtains a financial product or service. Accordingly, the final rule states, in § 313.4(d)(2), that a financial institution will satisfy the notice requirements when an existing customer obtains a new financial product or service if the institution's initial, revised, or annual notice (as appropriate) is accurate with respect to the new financial product or service.

Joint accountholders. The majority of comments on how to provide notice suggested that the final rule state that a financial institution is not obligated to provide more than one notice to joint accountholders. Several of these commenters noted that disclosure obligations arising from joint accounts are well settled under other rules, such as the regulations implementing the Equal Credit Opportunity Act (Regulation B, 12 CFR part 202,) and TILA. Under both Reg. B and Reg. Z, a financial institution is permitted to give only one notice. The authorities cited include requirements that the financial institution give disclosures, as appropriate, to the ''primary applicant'' if this is readily apparent (in the case of Reg. B; *see* 12 CFR 202.9(f)) or to a person ''primarily liable on the account'' (in the case of Reg. Z; *see* 12 CFR 226.5(b)).

The Commission agrees that a financial institution should be allowed to provide initial notices in a manner consistent with other disclosure obligations. There are also circumstances, however, where more than one of the joint account holders may want separate notices. Therefore, the final rule states in § 313.9 that the financial institution may send one notice, but must honor requests from one or more account holders for separate notices. Even absent a request, a financial institution may, in its discretion, provide notices to each party to the account. This situation might arise, for instance, when a financial institution does not want one opt out election to apply automatically to all joint accountholders (*see* discussion of how to provide opt out notices, below).

Mergers. A few commenters requested guidance on what notices are required in the event of a merger of two financial institutions or an acquisition of one financial institution by another. In such a situation, the need to provide new initial (and opt out) notices to the customers of the entity that ceases to exist will depend on whether the notices previously given to those customers accurately reflect the policies and practices of the surviving entity. If

they do, the surviving entity will not be required under the rule to provide new notices.

As was stated in the preamble to the proposed rule, a financial institution must maintain any protections that it represents it will provide in its privacy notices. Financial institutions must take appropriate measures to adhere to their stated policies and practices.

Section 313.5 Annual Privacy Notice to Customers 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 ''during the continuation'' of a customer relationship. The proposed rule implemented 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 proposed rule noted that provisions governing how to provide an initial notice also would apply to annual notices, and stated that a financial institution would not be required to provide annual notices to a customer with whom it no longer has a continuing relationship.

Several commenters requested that the final rule permit annual notices to be given each calendar year, instead of every twelve months. A variation suggested by a few commenters was to state that notices must be provided during each calendar year, with no more than 15 months elapsing between mailings. To clarify the extent of financial institutions' flexibility, the final rule retains the general rule requiring annual notices but then provides an example, in § 313.5(a)(2), stating that a financial institution may select a calendar year as the 12-month period within which notices will be provided and provide the first annual notice at any point in the calendar year following the year in which the customer relationship was established. The final rule also requires that a financial institution apply the 12-month cycle to its consumers on a consistent basis.

Several commenters suggested that a financial institution be permitted to make the annual notice available upon request only, particularly if there have been no material changes to the notice since it was last delivered or the customer has opted out. These commenters maintained that little value is added by providing customers with additional copies each year of the same information. Some suggested that financial institutions be permitted to provide a ''short-form'' annual notice, in which the institution informs its customers that there has been no change to its privacy policies and practices and that the customers may obtain a copy upon request.

The Commission has not amended the final rule to permit this approach, for two reasons. First, the Commission interprets the statute as contemplating complete disclosures annually to all customers during the duration of the customer relationship. Section 503 of the G-L-B Act states that ''not less than annually during the continuation of [a customer] relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer [*i.e.,* one with whom a customer relationship has been formed], . . . of such financial institution's policies and practices with respect to'' the information enumerated in the statute. The Commission believes that this provision contemplates a full set of disclosures to each customer once a year.

Second, the clarifications made in the final rule to the disclosure provisions make it clear that a financial institution is not required to provide a lengthy and detailed privacy notice to comply with the rule. Small institutions that do not share information with third parties beyond the statutory exceptions should be able to provide a short, streamlined notice. The rule also permits a financial institution to provide annual notices to customers over the institution's web site if the customer conducts transactions electronically and agrees to such disclosures (*see* additional discussion of this flexibility, below, in § 313.9). As a result, the final rule achieves much of the burden reduction sought by those requesting a short-form annual notice option.

Most of the remaining comments received in response to proposed § 313.5 addressed the sections governing when a customer relationship is terminated. Some noted that the examples used ''consumer'' when ''customer'' was appropriate, and the final rule is revised accordingly. A few commenters, including retailers and some whose business related to real estate transactions, stated that the example of no communication with a customer for twelve months should be amended to clarify that promotional materials would not be considered a communication about the relationship sufficient to reactivate a dormant or terminated customer relationship. These commenters generally suggested that the rule be tied to communications initiated by the customer. The Commission agrees that a communication that merely informs a person about, or seeks to encourage use of, a financial institution's products or services is not the type of communication that signifies an ongoing relationship. The final rule has been amended in § 313.5(b)(2)(vii) to reflect that the distribution of promotional materials will not prolong a customer relationship under the rule. The Commission disagrees, however, that the test should focus on whether there has been any customer-initiated contact, because there will be instances in which the customer will not initiate a contact with a financial institution within the relevant time period but nonetheless has an ongoing relationship.

Section 313.6 Information To Be Included in Initial and Annual Privacy Notices

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 proposed rule implemented section 503 by requiring a financial institution to provide information concerning:

- The categories of nonpublic personal information that a financial institution may collect;
- The categories of nonpublic personal information that a financial institution may disclose;
- The categories of affiliates and nonaffiliated third parties to whom a financial institution discloses nonpublic personal information, other than those to whom information is disclosed pursuant to an exception in section 502(e) of the G-L-B Act;
- The financial institution's policies with respect to sharing information about former customers;
- The categories of information that are disclosed pursuant to agreements with third party service providers and joint marketers and the categories of third parties providing the services;
- A consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties;
- Any disclosures regarding affiliate information sharing opt outs a financial

institution is providing under the FCRA; and

• The financial institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.

The Commission received a large number of comments concerning these requirements, with the majority of comments making the points summarized below.

Level of detail required. Many commenters offered the general observation that the level of detail that would be required under the proposed rule would result in lengthy, complicated, and ultimately confusing disclosures. These comments have led the Commission to clarify the level of detail that is required in a financial institution's initial and annual disclosures to contain.

Neither the Act nor this rule requires a financial institution to publish lengthy disclosures that identify with precision every type of information collected or disclosed, the name of every entity with whom the financial institution shares information, a complete description of the technical specifications of methods used by the institution to protect its customers' records, or the identity of each employee who has access to the records. Instead, the Commission has concluded that the statute, by focusing on ''categories'' of information and recipients of information, is intended to require notices that provide consumers with a general description of the third parties to whom a financial institution discloses nonpublic personal information, the types of information it discloses, and the other information about the institution's privacy policies and practices listed above. The Commission's intent is that the notice must be reasonably designed to be meaningful to consumers. The final rule, like the proposal, permits a financial institution to comply with these notice requirements by providing a description that accurately represents its privacy policies and practices. The Commission believes that in most cases the initial and annual disclosure requirements can be satisfied by disclosures contained in a tri-fold brochure.

To address commenters' concerns about the likelihood that consumers will not read long, detailed disclosures, the Commission has revised the examples of the disclosures set out in proposed § 313.6(e), which appears in the final rule at § 313.6(c), to clarify the level of detail that it thinks is appropriate under the G-L-B Act. Sample clauses have been provided in Appendix A to the rule, and guidance for certain institutions has been set out below in Section D. Because the examples are not exclusive, the final rule permits a financial institution to use categories different from those provided in the examples, thereby providing additional flexibility for financial institutions in complying with the disclosure requirements. In addition, the language in § 313.6(a) that precedes the items of information to be addressed in the initial notice has been amended to clarify that a financial institution is required only to address those items that apply to the institution. Thus, for instance, if a financial institution does not disclose nonpublic personal information to third parties, it may simply omit any reference to the categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information. The Commission has made these changes to clarify financial institutions' obligations under the statute and thereby eliminate unnecessary confusion.

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 Commission received conflicting suggestions relating to disclosures required about information provided to service providers and joint marketers. Some industry commenters suggested that the example in § 313.6(a)(5) required the same specificity as other disclosures and that it should be collapsed into § 313.6(a)(1–4). Some consumer advocates asked for more detail with respect to these disclosures, because consumers cannot opt out of them. The Commission believes that the example in § 313.6(a)(5) appropriately requires a ''separate statement'' on this point, and that this is sufficient to alert consumers about this practice. Therefore, it retains the example as proposed.

Short-form initial notice. The Commission has reconsidered the need to give consumers a copy of a financial institution's complete initial notice when there is no customer relationship. In these circumstances, the Commission believes that the objectives of the statute can be accomplished in a less burdensome way than was proposed and has exercised its exemptive authority as provided in section 504(b) to create an exception to the general rule that otherwise requires a financial institution to provide both the initial and opt out notices to a consumer before disclosing nonpublic personal information about that consumer to nonaffiliated third parties.

This exception is set out in § 313.6(d) of the final rule, which states that a financial institution may provide a ''short-form'' initial privacy policy notice along with the opt out notice to a consumer with whom the institution does not have a customer relationship. The short-form notice, along with the opt out notice, must clearly and conspicuously state that the disclosure containing information about the institution's privacy policies and practices is available upon request and provide one or more reasonable means by which the consumer may obtain a copy of the notice. This approach reflects the conclusion that consumers who do not become customers of a financial institution generally will have less interest in the privacy policies of that financial institution and will benefit from obtaining a concise, but meaningful, opt out notice that informs the consumer about the categories of their information the institution intends to disclose and the categories of nonaffiliated third parties that will receive the information. Consumers who are interested in the more complete privacy disclosures will be provided with a convenient means to obtain them.

Information about affiliate sharing. Another point made by several commenters in response to proposed § 313.6 was that the rule should not include a requirement that categories of affiliates with whom a financial institution shares information be included in the initial and annual notices. These commenters pointed out that the statute specifically requires disclosures of categories of nonaffiliated third parties only, and that the only statutorily mandated disclosures concerning affiliate sharing are disclosures required, if any, concerning affiliate sharing pursuant to section 603(d)(2)(A)(iii) of the FCRA.[33] These commenters concluded that the Commission, by expanding the disclosure requirements in the manner

[33] 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 the disclosure of that information. The information that can be disclosed to affiliates under this provision includes information from consumer reports. It also includes personal information provided directly by consumers to institutions in applications for financial products or services, such as information on income and assets.

prescribed in the proposed rule, would be exceeding its rulemaking authority and imposing unnecessary burdens on financial institutions.

The language and legislative history of section 503 support requiring disclosures of affiliate sharing beyond what may be required by the FCRA. First, section 503(b) does not state that the items listed therein are to be the only items set out in a financial institution's initial and annual disclosures. Instead, it uses the nonrestrictive phrase ''shall include'' when discussing the contents of the disclosures, thereby preserving flexibility for the Commission (which was expressly granted authority under section 503(a) to prescribe rules governing these notices) to require that additional items be addressed in the disclosures consistent with those specifically enumerated.

Second, section 503(a) provides that the financial institution shall provide in its initial and annual notices ''a clear and conspicuous disclosure * * * of such financial institution's policies and practices with respect to—(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 502, including the categories of information that may be disclosed; * * *.'' While the FCRA disclosures would be a subset of the disclosures required by section 503(a)(1), they may not be sufficient to fully satisfy that requirement.

Third, the legislative history of the G-L-B Act suggests that Congress intended for the disclosures to provide more information about affiliate sharing than what may be required under the FCRA.[34] That history underscores the Congressional intent of ensuring that individuals are given the opportunity to make informed decisions by reviewing the privacy policies and practices of financial institutions. The Commission believes that limiting the disclosures about affiliate sharing just to those disclosures required under the FCRA would frustrate that purpose.

Disclosures of the FCRA opt out right. Another frequent comment was that a financial institution should not be required to include FCRA disclosures in its annual notices. As previously discussed, 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. The proposed rule implemented 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 makes under section 603(d)(2)(A)(iii) of the FCRA. Several commenters pointed out that the FCRA requires disclosures of a consumer's right to opt out of affiliate sharing only once. They noted that the G-L-B Act states, in section 506(c), that nothing in the G-L-B Act is to be construed to modify, limit, or supersede the operation of the FCRA. The ''if any'' language of section 503(b)(4), read in the context of section 506, suggests that, since at most only one notice must be provided under the FCRA, section 503 should require only one FCRA disclosure under the privacy rule. The commenters concluded that, by requiring more notices than are required under the FCRA, the Commission would be violating this express preservation of the FCRA.

In order to comply with the requirement of the G-L-B Act that it disclose its policies and practices with respect to sharing information with affiliated and nonaffiliated third parties, a financial institution, must describe the circumstances under which it will be sharing information with affiliates. Clearly, the ability of consumers to opt out of affiliate information sharing under the FCRA affects a financial institution's policies and practices with respect to disclosing information to its affiliates. The Commission finds that failing to include this information and an explanation of how the opt out right may be exercised would make the disclosures incomplete. Thus, a financial institution must include this information in its initial and annual notices.

The commenters' reading of sections 503 and 506 is wrong. Section 503 does not distinguish between the disclosures to be provided in the initial notice from those to be provided in the annual notice. Thus, a plain reading of section 503 suggests that any disclosures that are required under the FCRA must be included in both the initial and annual notices.

The ''if any'' language is a recognition that not all institutions provide FCRA notices because not all institutions engage in the type of affiliate sharing covered by the FCRA. By requiring the FCRA notice to appear as part of the annual notice under the privacy rule, the Commission is not modifying, limiting, or superseding the operation of the FCRA; financial institutions will have exactly the same FCRA obligations following the effective date of the privacy rule as they had before. The only difference will be that, as is required by the G-L-B Act, a financial institution's initial and annual disclosures about its privacy policy and practices will need to reflect how the financial institution complies with the affiliate sharing provisions of the FCRA.

Disclosures of the right to opt out. Other commenters suggested that the final rule eliminate the requirement that the initial and annual notices contain disclosures about a consumer's right to opt out. These commenters pointed out that the statute does not specifically require these disclosures.

As previously discussed, section 503(a) of the statute requires a financial institution to disclose its policies and practices with respect to sharing information, both with affiliated and nonaffiliated third parties. Given that a financial institution's practices with respect to sharing nonpublic personal information with nonaffiliated third parties will be affected by the opt out rights created by the statute, an institution will need to describe these opt out rights in order to provide a complete disclosure that satisfies the statute.

Other comments. Many commenters expressed support for a number of the provisions in proposed § 313.6. For instance, several commenters noted their agreement with the approach of permitting a financial institution to state generally that it makes disclosures to nonaffiliated third parties ''as permitted by law'' to describe disclosures made pursuant to one of the exceptions. Others agreed with the proposed flexibility to allow a disclosure to be based on current and contemplated information sharing. In addition, the Commission received may requests for model forms of privacy notices. In light of these comments, the Commission has adopted proposed § 313.6 with changes as discussed above, plus stylistic changes to the material in § 313.6 that are intended to make the rule easier to read, and added the sample clauses in Appendix A.

Section 313.7 Form of Opt Out Notice to Consumers; Opt Out Methods

Paragraph (a) of proposed § 313.8 required that any opt out notice provided by a financial institution be clear and conspicuous and accurately explain the right to opt out. The

[34] *See, e.g.*, remarks of Sen. Gramm (noting that the privacy bill contains ''for the first time a full disclosure requirement. It requires every bank in America, when you open your account to tell you precisely what their policy is: Do they share personal financial information within the bank? Do they share it outside the bank?''), 145 Cong. Rec. S13786 (daily ed. Nov. 3, 1999); remarks of Sen. Hagel, *id.* at S13876 (''Financial institutions would be required to disclose their privacy policies to their customers on a timely basis. If customers do not believe adequate protections exist at their institution, they can take their business elsewhere.'').

proposed rule also required a financial institution to provide the consumer with a reasonable means by which to opt out, required a financial institution to honor an opt out election as soon as reasonably practicable, and stated that an opt out election survived until revoked by the consumer. The Commission received several comments in response to each of these provisions, addressing the application of these rules to joint accounts, the means by which an opt out right may be exercised, duration of an opt out, the level of detail required in the opt out notice, and the time by which an opt out election must be honored. These points are addressed below.

Joint accounts. Most of the commenters on this issue stated that a financial institution should have the option of providing one notice per account, regardless of the number of persons on the account. The Commission has added a new § 313.7(d) to address this issue. Under the final rule, a financial institution has the option of providing only one initial, annual, and opt out notice per account. However, if one or more of the joint account holders requests separate notices, the financial institution must honor that request. Even in instances where only one notice is provided, any of the accountholders must have the right to opt out. The final rule requires a financial institution to state in the opt out notice provided to a joint accountholder whether the institution will consider an opt out by a joint accountholder as an opt out by all of the associated accountholders or whether each accountholder is permitted to opt out separately.

Means of opting out. Another issue addressed by many commenters concerned the means by which consumers may opt out. Several suggested that a financial institution, after having provided reasonable means of opting out, should be able to require consumers to use those means exclusively. The Commission recognizes that a financial institution may not have trained personnel or systems in place to handle opt out elections at each point of contact between a consumer and financial institution. Assuming a financial institution offers one or more of the opt out means provided in the examples in the final rule or a means of opting out that is comparably convenient for a consumer, the institution may require consumers to opt out in accordance with those means and choose not to honor opt out elections communicated to the institution through alternative means. A new paragraph (iv) has been added to § 313.7(a)(2)(iv) to reflect this. However, as stated in § 313.7(a)(2)(iii)(A), a financial institution may not require a consumer to write his or her own letter in order to opt out.

Several commenters supported the alternative ways in which financial institutions could provide for consumers to opt out, especially the toll-free number set forth in § 313.8(a)(2)(ii)(D) in the Commission's proposal that was not included in the other Agencies' proposed rule. The Commission has retained that example in § 313.7(a)(2)(ii)(D) of the final rule, and the other Agencies have added the toll-free telephone number to their lists of examples. The Commission also received numerous comments indicating that one of the proposal's means of opting out, providing a self-addressed stamped envelope with a detachable card, was too burdensome. The Commission has, therefore, revised that example to provide for a reply form that contains the relevant address to facilitate the consumers ability to return it.

Duration of opt out. Several commenters questioned the practicality of the rule concerning duration of an opt out, as provided in § 313.8(e) of the proposal. These commenters noted that, under the proposal, a financial institution would be required to keep track of opt out elections forever. To illustrate their point, the commenters posited the example of a person who opts out during the course of establishing a customer relationship with a financial institution, terminates that relationship, and then establishes another customer relationship several years later, perhaps under a different name or with someone on a joint account. The commenters suggested that it would be more appropriate in these circumstances to treat the opt out election made in connection with the first relationship as applying solely to that relationship.

The Commission agrees. Thus, under the final rule, a financial institution is not required to treat an opt out election made by a customer in connection with a prior customer relationship as applying solely to the nonpublic personal information that the financial institution collected during, or related to, that relationship. That opt out will continue until the customer revokes it. However, if the customer relationship terminates and a new one is established at a later point, the financial institution must then provide a new opt out notice to the customer in connection with the new relationship and any prior opt out election does not apply to the new relationship.

Level of detail required in opt out notice. A few commenters expressed concern about the level of detail they perceived the proposed rule to require in an opt out notice. These commenters interpreted the statement in proposed § 313.8(a)(2) that a financial institution ''provides adequate notice . . . if [the institution] identifies all of the categories of nonpublic personal information that [the institution] discloses or reserves the right to disclose to nonaffiliated third parties as described in [§ 313.6]'' as requiring a more detailed disclosure of categories of nonpublic personal information and nonaffiliated third parties than is required in the initial and annual notices.

The Commission did not intend this result, and specifically referred to § 313.6 in the proposed opt out provision to address precisely the concern raised by these commenters. The disclosures in the initial and annual notices of the categories of nonpublic personal information being disclosed and the categories of nonaffiliated third parties to whom the information is disclosed will suffice for purposes of the opt out notices as well. If the opt out notice is a part of the same document that contains the disclosures that must be included in the initial notice, then the financial institution is not required to restate the same information in the opt out notice. In this instance, the rule requires only that the categories of nonpublic personal information the institution intends to share and the categories of nonaffiliated third parties with whom it will share are clearly disclosed to the consumer when the opt out and privacy notices are read together.

One commenter suggested that, while a financial institution should have the option of providing an opt out notice that is sufficiently broad to cover anticipated disclosures, the financial institution also should be permitted to provide a customer who already has opted out with a new opt out notice in connection with a new financial product or service and, if the consumer does not opt out a second time, be free to disclose nonpublic personal information obtained in connection with that financial product or service to nonaffiliated third parties. The Commission believes that a financial institution should be permitted the flexibility to provide opt out notices that are either clearly limited to specific types of nonpublic personal information and types of nonaffiliated third parties, or that are more broadly worded to anticipate future disclosure plans. However, if a consumer opts out after

receiving an opt out notice from a financial institution that is broad enough to cover the new type of information sharing desired by that institution, the failure of the consumer to opt out again does not revoke the earlier opt out election.

Time by which opt out must be honored. Under the proposal, a financial institution is directed to comply with an opt out election ''as soon as reasonably practicable.'' A large number of comments asked the Commission to clarify in the final rule how long a financial institution has after receiving an opt out election to cease disclosing nonpublic personal information to nonaffiliated third parties. Suggestions for a more precise standard ranged from mandating that a financial institution stop disclosing information immediately to a mandatory cessation within several months of receiving the opt out. As was the case with other suggestions for bright-line standards in different contexts, the Commission believes that it is appropriate to retain a more general rule in light of the wide range of practices throughout the various financial institutions within its jurisdiction. A potential drawback of a more prescriptive rule is that an institution might use the standard as a safe harbor in all instances and thus fail to honor an opt out election as early as it is otherwise capable of doing. Another drawback is that a standard that is set in light of current industry practices and capabilities may become outmoded as advances in technology increase efficiency. The Commission therefore declines to adopt a more rigid standard and instead retains the rule as set out in § 313.7(e) of the final rule.

For the reasons stated above, the Commission adopts, in § 313.7, the rule governing the form of opt out notices and methods of opting out as discussed above. This section contains other stylistic changes to what was proposed in order to make the final rule easier to read.

Section 313.8 Revised Privacy Notices

The proposed rule, in § 313.8(c) (''Notice of change in terms''), prohibited a financial institution (directly, or through its affiliates) from disclosing nonpublic personal information about its consumers to nonaffiliated third parties unless the institution first provided a copy of its privacy notice and opt out notice. The proposal also required that these notices be accurate when given. Thus, if an institution wants to disclose nonpublic personal information in a way that is not accurately described in its notices, the institution would be required under the proposed rule to provide new notices before making the disclosure in question.

The only comments relating to these requirements received by the Commission posited that a revised notice should be required only upon material changes. Section 313.8(a)(i) addresses this point—no new notice is required if the original notice ''accurately describes'' the institution's policies. Accordingly, the Commission adopts the rule as proposed, but places the relevant provisions in a separate section (§ 313.8, ''Revised privacy notices'') in the final rule for emphasis. The final rule sets out examples in § 313.8(b) of when a new notice would, and would not, be required.

Section 313.9 Delivering Privacy and Opt Out Notices

The proposed rules governing delivery of initial, annual, and opt out notices were set out in proposed §§ 313.4(d), 313.5(b), and 313.8(b), respectively. Given the substantial similarities between the three sets of rules, the Commission has decided to combine the rules in one section in order to make it easier for the reader. Accordingly, the final rule states these rules in § 313.9.

The general rule requires that notices be provided in a manner so that each consumer can reasonably be expected to receive actual notice in writing, or, if the consumer agrees, electronically. The Commission received a number of comments on the various provisions governing delivery, as discussed below.

Posting initial notices on a web site. A few commenters suggested that a financial institution be allowed to deliver initial notices simply by posting its notice on the institution's web site. Some of them criticized the example in proposed § 313.4(d)(5)(C) that required the consumer to acknowledge receipt of an electronic communication as tantamount to an ''opt-in'' provision; conversely, at least one consumer representative vigorously contended that it was essential that the consumer affirmatively respond in this situation because computer literacy cannot be presumed from the use of a web site.

There will be instances when a notice on a web site may be delivered in a way that will enable the financial institution to reasonably expect that the consumer will receive it. The final rule retains, as an example of one way to comply with the rule, the posting of a notice on a web site and requiring a consumer to acknowledge receipt of the notice as a step in the process of obtaining a financial product or service. *See* § 313.9(b)(1)(iii). However, the mere posting of a notice on a web site would not be sufficient in all cases for the financial institution to reasonably expect its consumers to receive the notice. Accordingly, the Commission does not view the limited acknowledgment of receipt in this context as equivalent to an opt in requirement.

Posting annual notices on a web site. Several commenters requested that a privacy notice posted by a financial institution on its web site be deemed to satisfy the annual notice requirement, at least for customers who agree to receive notices on the institution's web site. The final rule contains a new § 313.9(c)(i) to clarify that a financial institution may reasonably expect that a customer who uses the institution's web site to access financial products or services will receive actual notice if the customer has agreed to accept notices at the institution's web site and the financial institution posts a current notice of its privacy policies and practices continuously and in a clear and conspicuous manner on the web site.

The Commission views it as appropriate to post the annual notice on the web site only where the customer is in a relationship with the financial institution that is conducted almost entirely at the web site and where the customer has explicitly agreed to receive all of its notices and financial information at the web site. Moreover, the financial institution must position any link or links to the privacy policy such that they are evident to the customer wherever the customer may go on the web site to conduct transactions or obtain information. In those circumstances, the Commission agrees that it is appropriate to provide annual notices in this way for customers who conduct transactions electronically and agree to accept notices on a web site. This will reduce burden on financial institutions while ensuring that customers who transact business electronically will have access to institutions' privacy policies and practices.

Disclosures to customers requesting no communication. Several commenters suggested the Commission clarify in the final rule how the disclosure obligations may be met in the case of a customer who requests that the institution refrain from sending information about the customer's relationship. These commenters stated that, in this case, the customer's request should be honored.

The Commission agrees. When a customer provides explicit instructions for a financial institution not to communicate with that customer, the

Commission believes that the request should be honored. The final rule clarifies, in § 313.9(c)(ii), that financial institutions need not send notices to a customer who requests no communication, provided that a notice is available upon request.

Reaccessing a notice. A few commenters stated that the requirement that a privacy policy be provided in a way that enables a customer to either retain or reaccess the notice should clarify that the rule obligates a financial institution to make available only the privacy policy currently in effect. These commenters were concerned about the potential for confusion and the burden stemming from a rule that would require a financial institution to make available every version of its privacy policies. The Commission agrees that it is appropriate to require only that the current privacy policy be made available to someone seeking to obtain it after having received the initial notice, and has revised the final rule accordingly in § 313.9(e)(2)(iii).

Joint notices. Other commenters requested that the rule clarify that the privacy policies and practices of several different affiliated financial institutions may be described on a single notice. Further, commenters requested that the final rule address whether affiliated financial institutions, each of whom has a customer relationship with the same consumer, may elect to send only one notice to the consumer on behalf of all of the affiliates covered by the notice and have that one notice satisfy the disclosure obligations under § 313.4 of each affiliate. Financial institutions should be able to combine initial disclosures in one document. The Commission also believes that it is appropriate to permit financial institutions that prepare a combined initial or annual notice to give, on a collective basis, a consumer only one copy of the notice. The final rule reflects this flexibility, in § 313.9(f). The notice must be accurate for all financial institutions using the notice, and must identify by name each of the institutions. The Commission also notes that financial institutions that provide one combined notice must be capable of keeping track of whether a consumer has opted out in order to ensure that disclosures are made in accordance with whatever opt out instructions a consumer provides after having received the joint notice.

Section 313.10 Limits on Disclosure of Nonpublic Personal Information to Nonaffiliated Third Parties

Section 502(a) of the G-L-B Act generally prohibits a financial institution, directly or through its affiliates, 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 implemented these provisions by requiring a financial institution to give the consumer the initial notice required by § 313.4, the opt out notice required by § 313.8, and a reasonable opportunity to opt out.

Most of the comments addressing these requirements focused on the question of what is a reasonable opportunity to opt out. Suggestions ranged from a financial institution having the right to begin sharing information immediately (when the opt out and initial notices are provided as part of a transaction being conducted electronically, such as might be the case in an ATM transaction) up to a mandatory delay of 120 days from the time the notices are provided.

The wide variety of suggestions underscores the appropriateness of a more general test that avoids setting a mandatory waiting period applicable in all cases. For isolated transactions where a financial institution intends to disclose nonpublic personal information that it obtains through an electronic transaction and the consumer is provided a convenient means of opting out as part of the transaction, it would be reasonable not to force the financial institution to wait a set period of time before sharing the information. Thus, the example in § 313.10(a)(3)(iii) provides flexibility. For other opt out notices that are provided by mail, the Commission believes it is appropriate to allow the consumer additional time. In these latter instances, the Commission considers it reasonable to permit the consumer to opt out by mailing back a form, by calling a toll-free number, or by any other reasonable means within 30 days from the date the opt out notice was mailed. *See* § 313.10(a)(3)(i). The final rule also provides an example of a reasonable opportunity for opting out in connection with accounts opened on-line. *See* § 313.10(a)(3)(ii). However, rather than try to anticipate every scenario and establish a time frame that would accommodate each, the rule simply provides that the consumer must be given a reasonable opportunity to opt out and then provide a few illustrative examples of what would be reasonable in different contexts.

Other comments pointed out that proposed § 313.7(a)(3)(i), which is § 313.10(a)(3)(i) of the final rule, inappropriately implied that the opportunity to opt out by mail is available only when a consumer has a customer relationship with the financial institution. The final rule deletes the reference to a customer relationship in that section to avoid that implication.

Section 313.11 Limits on Redisclosure and Reuse of Information

Section 502(c) of the G-L-B 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 both the financial institution and the third party, unless the disclosure would be lawful if made directly by the financial institution. The proposed rule implemented section 502(c) by imposing limits on redisclosure that apply both to a financial institution that receives information from a nonaffiliated financial institution and to any nonaffiliated third party that receives nonpublic personal information from a financial institution. The proposed rule also imposed limits on the ability of financial institutions and nonaffiliated third parties to reuse nonpublic personal information they receive. As noted in the preamble to the proposed rule, sections 502(b)(2) and 502(e) permit disclosures of nonpublic personal information for specific purposes. The Commission sought comment on whether the final rule should limit the ability of an entity that receives nonpublic personal information pursuant to an exception to use that information only for the purpose of that exception. The Commission also sought comment on what the term ''lawful'' means in the context of section 502(c), and whether a recipient of nonpublic personal information could ''lawfully'' disclose information if the disclosure complied with a notice provided by the institution that made the disclosure initially. Finally, the Commission invited 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.

The Commission received many comments in response to this proposed section. A few opined that the Commission would exceed its rulemaking authority if the final rule were to retain the limits on reuse of information, given that section 502(c) expressly addresses only redisclosures and not reuse. Most comments concerning proposed § 313.12 stated that financial institutions should not have to monitor compliance with the redisclosure and reuse provisions of the rule, although these commenters said that financial institutions typically will contractually limit the recipient's ability to reuse information for purposes other than those for which the information was disclosed. The Commission also received comments from consumer reporting agencies, individual reference services, private investigators, and direct marketers stating that consumer reporting agencies should be able to continue their practice of selling ''credit header'' information that they obtain from financial institutions, as well as some comments stating that the Commission should clarify that the rules prohibit the continued distribution of such information by consumer reporting agencies. These issues are addressed below.

Limits on reuse. Those critical of imposing limits on reuse believe that Congress, by addressing limits on redisclosures in section 502(c), provided the only limits that may be imposed on what a recipient of nonpublic personal information can do with that information. The Commission disagrees. Section 502(c) is silent on the question of reuse, making it necessary to look to the overall purposes of the statute to determine whether the Commission should impose limits on the ability of nonaffiliated third parties to reuse nonpublic personal information that they receive from a financial institution. The Act makes it appropriate to impose limits on reuse, depending on whether the information was obtained pursuant to one of the exceptions in section 502(e) of the G-L-B Act (as implemented by §§ 313.14 and 313.15 of the final rule).

When disclosures are made to nonaffiliated third parties in connection with one of the purposes set out in section 502(e), those disclosures are exempt from the notice and opt out protections altogether. A customer has no right to prohibit those disclosures or even to know more than that the disclosures are being made ''as permitted by law.'' A consumer who does not establish a customer relationship is not even put on notice that the disclosures are made as permitted by law, because the consumer is not entitled to any privacy or opt out notice. The only protection afforded by the statute for disclosures made under section 502(e) is the limited nature of the exceptions. It would be inappropriate to undermine the key privacy requirements of the Act that ensure a consumer can generally control the disclosure of his or her nonpublic personal information by allowing the recipient of nonpublic personal information under the section 502(e) exception to reuse the information for any purpose, including marketing.

By contrast, when a consumer decides not to opt out after being given adequate notices and the opportunity to do so, that consumer has made a decision to permit the sharing of his or her nonpublic personal information with the categories of entities identified in the financial institution's notices. The consumer's primary protection in the case of a disclosure falling outside the section 502(e) exceptions comes from receiving the mandatory disclosures and the right to opt out. The statute provides only the additional protection in section 502(c), restricting a recipient's ability to redisclose information to entities that are not affiliated with either the recipient or the financial institution making the disclosure initially. Thus, if a consumer permits a financial institution to disclose nonpublic personal information to the categories of nonaffiliated third parties that are described in the institution's notices, recipients of that nonpublic personal information appear authorized under the statute to make disclosures that comply with those notices.

To implement this statutory scheme, the Commission has retained a limit on reuse in addition to the limit on redisclosures. The limits on redisclosure and reuse that apply to recipients of information and their affiliates will vary, depending on whether the information was provided pursuant to one of the section 502(e) exceptions.

For nonpublic personal information provided pursuant to section 502(e), a financial institution receiving the information may disclose the information to its affiliates or to affiliates of the financial institution from which the information was received. It may also disclose and use the information pursuant to an exception in §§ 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which the institution received the information. Therefore, the financial institution's affiliates may disclose and use the information, but only to the extent permissible for the financial institution under those exceptions.

For nonpublic personal information provided *outside* one of the section 502(e) exceptions (*i.e.*, where a customer or consumer has not opted out), the financial institution receiving the information may disclose the information to its affiliates or to the affiliates of the financial institution that made the initial disclosure. It may also disclose the information to any other person, if the disclosure would be lawful if made directly by the financial institution from which the information was received. This would enable the receiving institution to redisclose information pursuant to one of the section 502(e) exceptions. It also would permit the receiving institution to redisclose information in accordance with the opt out and privacy notices given by the institution making the initial disclosures, as limited by any opt out elections received by that institution. The affiliates of a financial institution that receives nonpublic personal information may disclose only to the extent that the financial institution may disclose the information.

These same general rules apply to a *non-financial institution* third party that receives nonpublic personal information from a financial institution. Thus, the third party receiving the information pursuant to one of the section 502(e) exceptions may disclose the information to its affiliates or to the affiliates of the financial institution that made the disclosure. The third party also may disclose and use the information pursuant to one of the section 502(e) exceptions as noted in the rule. The affiliates of the third party may disclose and use the information only to the extent permissible for the third party. If the third party receives the information from a financial institution outside one of the section 502(e) exceptions, the third party may disclose to its affiliates or to the affiliates of the financial institution. It may also disclose to any other person if the disclosure would be lawful if made by the financial institution. The third party's affiliates may disclose and use the information to the same extent permissible for the third party.

To summarize, in cases where an entity receives information outside of one of the section 502(e) exceptions, that entity will in essence ''step into the shoes'' of the financial institution that made the initial disclosures. Thus, if the financial institution made the initial disclosures after representing to its consumers that it had carefully screened the entities to whom it intended to

disclose the information, the receiving entity must be able to comply with those representations. Otherwise, the subsequent disclosure by the receiving entity would not be in accordance with the notices given to consumers and would not, therefore, be lawful. Even if such representations do not prevent the recipient from redisclosing the information, the recipient's ability to redisclose will be limited by whatever opt out instructions were given to the institution making the initial disclosures and by whatever new opt out instructions are given after the initial disclosure. The receiving entity, therefore, must have procedures in place to continually monitor the status of who opts out and to what extent. Given these practical limitations on the ability of a recipient to disclose pursuant to another institution's privacy and opt out notices, redisclosure of information is most likely to arise under one of the section 502(e) exceptions (as implemented by §§ 313.14 and 313.15 of the final rule).

Monitoring third parties. The final rule does not impose a general duty on financial institutions to monitor third parties' use of nonpublic personal information provided by the institutions. Obligations to do so may arise in other contexts, however. For instance, some of the commenters who requested that the Commission not impose such a duty stated that they have contracts in place that limit what the recipient may do with the information. Also, the limits on reuse as stated in the final rule provide a basis for an action to be brought against an entity that violates those limits.

Redisclosure by consumer reporting agencies. Comments regarding the availability of credit header information [35] from consumer reporting agencies addressed not only the reuse and redisclosure provisions, but also the definition of nonpublic personal information (*see* § 313.3(n, o, p) above), the exception in § 313.15(a)(5), and the operation of the Fair Credit Reporting Act (*see* § 313.16 below). For clarity, the Commission addresses the credit header issue here, with reference as appropriate to other provisions of the final rule.

The definition of nonpublic personal information dictates that all of the information a financial institution provides to a consumer reporting agency is nonpublic personal information: ''Any list, description or other grouping of consumers (*and publicly available information pertaining to them*) that is derived using any personally identifiable financial information * * *.'' (§ 313.3(n)(1)(ii)(emphasis added).) The financial institution is permitted under § 313.15(a)(5) to disclose this nonpublic personal information, without giving the consumer notice and the opportunity to opt out, ''[t]o a consumer reporting agency * * *.'' That same exception states that the notice and opt out provisions do not apply to nonpublic personal information ''from a consumer report reported by a consumer reporting agency.''

The Commission recognizes that § 313.15(a)(5) permits the continuation of the traditional consumer reporting business, whereby financial institutions report information about their consumers to the consumer reporting agencies and the consumer reporting agencies, in turn, disclose that information in the form of consumer reports to those who have a permissible purpose to obtain them. Despite a contrary position expressed by some commenters, this exception does not allow consumer reporting agencies to redisclose the nonpublic personal information it receives from financial institutions other than in the form of a consumer report. Therefore, the exception does not operate to allow the disclosure of credit header information to individual reference services, direct marketers, or any other party that does not have a permissible purpose to obtain that information as part of a consumer report.[36]

Disclosure by a consumer reporting agency of the nonpublic personal information it receives from a financial institution pursuant to the exception, other than in the form of a consumer report, is governed by the limitations on reuse and redisclosure in § 313.11, discussed above in ''Limits on reuse.'' Those limitations do not permit consumer reporting agencies to disclose credit header information that they received from financial institutions to nonaffiliated third parties. Some commenters suggested that the information loses its status as ''nonpublic personal information'' when the consumer reporting agencies combine it with other information in their databases. The Commission does not agree. The information is disclosed to the consumer reporting agencies as nonpublic personal information and it retains that status regardless of how the consumer reporting agency stores or redisclosures that data.

Several commenters stated that the Fair Credit Reporting Act operates to allow consumer reporting agencies to disclose credit header information and, therefore, any prohibition on the sale of credit header information violates section 506 of the G–L–B Act, which states that ''nothing in [Title V of the G-L-B Act] shall be construed to modify, limit, or supercede the operation of the [FCRA].'' The Commission does not agree. To the extent credit header information is not a consumer report, it is not regulated by the FCRA and a prohibition on its disclosure by a consumer reporting agency consistent with the statutory scheme of the G-L-B Act in no way modifies, limits or supercedes the operation of the FCRA.[37]

At least one commenter requested that the Commission make use of the authority granted to it under section 504(b) of the G-L-B Act to provide for an exception to the reuse and redisclosure limitations that would allow consumer reporting agencies to sell credit header information. The Commission does not believe that such an exception is consistent with the privacy provisions of the Act, which function to protect a consumer's nonpublic personal information from widespread distribution without notice and the opportunity for the consumer to opt out. An exception that allows a consumer reporting agency to redisclose that information where there has been no notice to the consumer and no opportunity for the consumer to direct that the information not be disclosed works at cross purposes with the Act. The Commission, therefore, declines to adopt such an exception.

If consumer reporting agencies receive credit header information from financial institutions outside of an exception, the limitations on reuse and redisclosure may allow them to continue to sell that information. This could occur if the originating financial institutions disclose in their privacy policies that they share consumers' nonpublic personal information with consumer reporting agencies, and provide consumers with the opportunity to opt out. Then, like any other nonaffiliated third party that receives information outside of an exception, the consumer

[35] ''Credit header'' information was traditionally defined to include identifying information such as name, address, telephone number, social security number, mother's maiden name, and age. However, the Commission's recent decision in *In re Trans Union,* Docket No. 9255 (Feb. 10, 2000), *appeal docketed,* No. 00–1141 (D.C. Cir. Apr. 4, 2000), determined that age is a ''consumer report'' and can be disclosed only pursuant to a permissible purpose under Section 604 of the Fair Credit Reporting Act.

[36] Section 608 of the Fair Credit Reporting Act does allow consumer reporting agencies to furnish a consumer's name, address, former addresses, places of employment, and former places of employment to a governmental agency.

[37] To the extent that previously-considered credit header information is now deemed consumer report information (*i.e.,* age), the FCRA provides requirements and protections in addition to those provided under the G-L-B Act.

reporting agency can redisclose that information consistent with the originating financial institutions' privacy policies and subject to applicable consumer opt out directions.

Section 313.12 Limits on Sharing 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, 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.'' Proposed § 313.13 applied this statutory prohibition to disclosures made directly or indirectly by a financial institution and sought comment on whether one or more exceptions to the flat prohibition should be created.

The Commission received many comments from people who suggested that various exceptions be created, as well as people who believe that a flat prohibition is necessary to protect consumers from unscrupulous practices. After considering the suggestions from all of the commenters addressing this issue, the Commission has decided, pursuant to its authority under 504(b), to modify proposed § 313.13 by (a) adding two exceptions that allow financial institutions to engage in legitimate, routine business practices and that are unlikely to pose a significant potential for abuse and (b) clarifying that the prohibition does not apply in two circumstances frequently mentioned in the comments. These exceptions and clarifications are discussed below.

Disclosures to a financial institution's agent or service provider. Many financial institutions noted that they use agents or service providers to conduct marketing on the institution's behalf. This might occur, for instance, when a mortgage lender instructs a service provider that assists in the delivery of monthly statements to include a ''statement stuffer'' with the statement informing consumers about a financial product or service offered by the institution. The Commission recognizes the need to disclose account numbers in this instance, and believe that there is little risk to the consumer presented by such disclosure.

Similarly, the Commission recognizes that a financial institution may use agents to market the institution's own financial products and services. Commenters advocating that the final rule exclude disclosures to agents stated that the agents effectively act as the financial institution in the marketing of the institution's financial products and services. These commenters suggested that there was no more reason to preclude sharing the account numbers with an agent hired to market the institution's financial products and services than there would be to preclude sharing between two departments of the same institution. The Commission is concerned, however, about the possibility of transactions being consummated by a financial institution's agent who may be engaging in practices contrary to the institution's instructions. While the Commission recognizes that a financial institution frequently will use agents to assist it in marketing its products, a consumer's protections are potentially eroded by allowing agents to have access to a consumer's account. Accordingly, an exception in § 313.12(b)(1) will permit disclosures of account numbers by a financial institution to an agent for the purpose of marketing the financial institution's financial product or services, but has qualified that exception by stating that the agent has no authority to make charges to the account.

Private label credit cards and affinity programs. Many commenters stated that the final rule should not prevent the disclosure of account numbers in the situation where a consumer chooses to participate in a private label credit card program or other affinity program. Under these programs, a consumer typically will be offered certain benefits, often by a retail merchant, in return for using a credit card that is issued by a particular financial institution. The commenters suggested that, in the example of an affinity program, the consumer understands the need for the merchant and financial institution to share the consumer's account number. The Commission agrees that this type of disclosure is appropriate and does not create a significant risk to the consumer. Accordingly, § 313.12(b)(2) has been added to the final rule to exclude the sharing of account numbers where the participants are identified to the consumer at the time the consumer enters into the program.

Encrypted numbers. Many commenters urged the Commission to exercise its exemptive authority to permit the transmission of account numbers in encrypted form. Several commenters noted that encrypted account numbers and other internal identifiers of an account are frequently used to ensure that a consumer's instructions are properly executed and that the inability to continue using these internal identifiers would increase the likelihood of errors in processing a consumer's instructions. These commenters also point out that if internal identifiers may not be used, a consumer would need to provide an account number in order to ensure proper handling of a request, which would expose the consumer to a greater risk than would the use of an internal tracking system that preserves the confidentiality of a number that may be used to access the account.

The Commission believes an encrypted account number without the key is something different from the number itself and thus falls outside the prohibition in section 502(d). In essence, it operates as an identifier attached to an account for internal tracking purposes only. The statute, by contrast, focuses on numbers that provide *access* to an account. Without the key to decrypt an account number, an encrypted number does not permit someone to access an account.

In light of the statutory focus on access numbers, and given the demonstrated need to be able to identify which account a financial institution should debit or credit in connection with a transaction, the Commission has included a clarification in § 313.12(c)(1) of the final rule stating that an account number, or similar form of access number or access code, does not include a number or code in an encrypted number form, as long as the financial institution does not provide the recipient with the means to decrypt the number. Consumers will be adequately protected by disclosures of encrypted account numbers that do not enable the recipient to access the consumer's account.

Definition of ''transaction account.'' Several commenters suggested that the final rule clarify that accounts to which no charge may be posted are not covered by the prohibition against disclosing account numbers. These commenters frequently cited mortgage loan accounts as typical of those that should fall outside the scope of the prohibition. The Commission agrees with the principle behind these suggestions. However, there have been instances in which a borrower's monthly payments on a mortgage loan have been increased in connection with the marketing of a financial product or service without the borrower's knowledge or permission. Accordingly, the final rule clarifies in § 313.12(c)(2) that a transaction account is an account, other than a deposit account or a credit card account, to which third parties can initiate charges.

If it would be possible, for instance, for a third party marketer to initiate a charge to a mortgage loan account, then the final rule would prohibit the disclosure of that account number to the marketer.

Section 313.13 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 rule 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. 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 ''fully discloses'' to the consumer that it will provide this information to the nonaffiliated third party before the information is shared and enters into a contract with the third party that requires the third party to maintain the confidentiality of the information. As noted in the proposed rule, 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 invited comment on whether the statute would prohibit the sharing of aggregate data without personal identifiers and whether additional requirements should be imposed on the agreements to address, for instance, reputation risk and legal risk for a financial institution entering into such an agreement.

The majority of the comments on this exception expressed concern that routine servicing agreements between a financial institution and, for instance, a loan servicer would be subject to the requirements of proposed § 313.9, which appears as § 313.13 in the final rule. These commenters consistently pointed out that section 502(e) of the G-L-B Act contains several exceptions for the sharing of information by a financial institution that is necessary to permit a third party to perform services for a financial institution. The commenters requested clarification that disclosures made pursuant to one of the section 502(e) exceptions are not subject to the requirements imposed on disclosures made pursuant to section 502(b)(2) of the G-L-B Act. The Commission agrees that when a disclosure may be made under section 502(e), the Act permits that disclosure without first complying with the requirements of section 502(b)(2).

A related issue is whether a financial institution must satisfy the disclosure obligations of section 502(b)(2) and have a confidentiality agreement in the case of a service provider that is performing an activity governed by section 502(b)(2) (*i.e.,* those that are not covered by one of the section 502(e) exceptions). Several commenters maintained that those requirements apply only to joint marketing agreements and that it is illogical to impose a set of requirements on disclosures to the section 502(b)(2) service providers when no such requirements are imposed on the section 502(e) service providers. The Commission believes, however, that a plain reading of section 502(b)(2) leads to that result.[38] The Commission reads the phrase ''if the financial institution fully discloses * * *'' as used in section 502(b)(2) as modifying the phrase ''[t]his subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, * * *'' The Commission thus has concluded that any disclosure to a service provider not covered by section 502(e) must satisfy the disclosure and written contract requirements of section 502(b)(2).

Several other commenters addressed the question of whether the rule should include safeguards beyond those provided by the statute to protect a financial institution from the risks that can arise from agreements with third parties. Most suggested that safety and soundness concerns were more appropriately addressed in a forum other than a rule designed to protect consumers' financial privacy. Others opined that financial institutions did not need the rule to mandate certain protections on their behalf. The Commission has concluded that the protections set out in the statute, as implemented by § 313.13(a)(1)(ii), are adequate for purposes of the privacy rule. Those protections require a financial institution to provide the initial notice required by § 313.4 of the final rule as well as enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the financial institution disclosed the information, including use under an exception in §§ 313.14 or 313.15 in the ordinary course of business to carry out those purposes. These limitations will preclude recipients from sharing a consumer's nonpublic personal information pursuant to a chain of third party joint marketing agreements.

Several commenters asked whether a financial institution would have to modify existing contracts with third parties to comply with the rule. The Commission believes that a balance must be struck that minimizes interference with existing contracts while preventing evasions of the regulation. To achieve these goals, the final rule states, in § 313.18(c), that contracts in effect as of July 1, 2000 must be brought into compliance with the provisions of § 313.13 by July 1, 2002. For the reasons expressed above, the Commission has adopted the provisions that were set out in § 313.9 of the proposal, with the changes noted above, as § 313.13 of the final rule.

Section 313.14 Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions

As previously discussed, 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. Proposed § 313.10 implemented those exceptions by restating them with only stylistic changes that were intended to make the exceptions easier to read. The preamble to that proposed section noted that the exceptions set out in proposed § 313.10 (as well as the exceptions set out in § 313.11 of the proposal) 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.

[38] Section 502(b)(2) states, in relevant part, that the opt out provision: ''shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated 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 joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

The Commission received several comments from institutions pointing out that, by deleting the statutory phrase ''in connection with'' from the exceptions for information shared (a) to service or process a financial product or service requested by the consumer or (b) to maintain or service a customer account, the Commission narrowed the application of the exception. The Commission did not intend this result and has changed the final rule accordingly. *See* § 313.14(a).

Several other commenters requested that the final rule specifically state that certain services, such as those provided by attorneys, appraisers, financial planners, and debt collectors (as appropriate), are ''necessary'' to effect, administer, or enforce a transaction, as that term is used in paragraph (a) and defined in paragraph (b) of proposed § 313.10. Others cited examples of entities seeking to verify funds availability or obtain loan payoff information as instances where a disclosure would fall within the exceptions described in proposed § 313.10. The Commission believes that disclosures to these types of professionals and under the circumstances posited by the commenters may be necessary to effect, administer, or enforce a transaction in a given situation. However, the Commission has not listed specific types of disclosures in the regulation as necessarily falling within the scope of the exception because such a general statement could be applied inappropriately to shelter disclosures that, in fact, are not necessary to effect, administer, or enforce a transaction.

Other commenters suggested that the final rule clarify, in situations where a financial institution uses an agent to provide services to a consumer, that the consumer need not have directly requested or authorized the service provider to provide the financial product or service but may request it from the principal instead. The Commission agrees that the communication may be between the consumer and the service provider and notes that the rule governing agents as set out in the definition of ''consumer'' above, provides the flexibility sought by the commenters. Briefly stated, an individual is not a consumer of an entity that is acting as agent for another financial institution in connection with that financial institution's providing a financial product or service to the consumer.

Section 313.15 Other Exceptions to Notice and 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 set out those exceptions for disclosures that are not made in connection with the administration, processing, servicing, and sale of a consumer's account and made stylistic changes to the statutory language intended to clarify the exceptions. The proposal also provided an example of the consent exception in the context of a financial institution that has received an application from a consumer for a mortgage loan informing a nonaffiliated insurance company that the consumer has applied for a loan. The Commission invited comment on whether safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion.

Several commenters responded to the request for comment on whether the consent exception should include safeguards, such as a requirement that the consent be written, be indicated by a signature on a separate line, or automatically terminate after a certain period of time. Of these, some favored the additional safeguards discussed in the proposal, while others maintained that such precautions are unnecessary. Several suggested that the consent exception include a provision noting that participation in a program where a consumer receives ''bundled'' products and services (such as would be the case, for instance, in an affinity program) necessarily implies consent to the disclosure of information between the entities that provide the bundled products or services. Others suggested that certain terms and conditions be imposed on any consent agreement, such as a time by which the financial institution must stop disclosing nonpublic personal information once a consent is revoked.

The Commission has declined to elaborate on the requirements for obtaining consent or the consumer safeguards that should be in place when a consumer consents. The resolution of this issue is appropriately left to the particular circumstances of a given transaction. Any financial institution that obtains the consent of a consumer to disclose nonpublic personal information should take steps to ensure that the limits of the consent are well understood by both the financial institution and the consumer. If misunderstandings arise, consumers may have means of redress, such as in situations when a financial institution obtains consent through a deceptive or fraudulent practice. Moreover, a consumer may always revoke his or her consent. In light of the safeguards already in place, the Commission has decided not to add safeguards to the consent exception.

Many commenters offered specific suggestions for additional exceptions or amendments to the proposed exceptions. In many cases, the suggestions are accommodated elsewhere in the regulation (such as is the case, for instance, for exceptions to permit (a) verification of available funds or (b) disclosures to or by appraisers, flood insurers, attorneys, insurance agents, or mortgage brokers to effect a transaction). In other cases, the suggestions are inconsistent with the statute (as is the case, for instance, with one commenter's suggestion that the Commission completely exempt a financial institution from all of the statute's requirements if the institution makes no disclosures other than what is permitted by section 502(e)). Accordingly, the Commission has retained, in § 313.15, the statement of the exceptions as proposed and invites interested parties to seek clarifications as necessary in their particular circumstance. See 16 CFR pt. 1.

Section 313.16 Protection of the Fair Credit Reporting Act

Section 506 of the G-L-B Act 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 of the G-L-B Act 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 whether information is transaction or experience information under section 603 of the FCRA. Proposed § 313.14 implemented section 506(c) of the G-L-B Act by restating the statute, making only minor stylistic changes intended to make the rule clearer.

Comments about this provision focused mainly on whether the Commission, by requiring annual notice of a consumer's right to opt out under the FCRA, was modifying, limiting, or superseding the operation of the FCRA. For the reasons explained in the discussion of § 313.6, above, the annual disclosure mandated by the G-L-B Act does not affect the obligations imposed by the FCRA.

Other commenters suggested that this section protects the ability of consumer reporting agencies to disclose credit header information to unaffiliated third parties. As discussed in § 313.11 above, the Commission disagrees with this position. Finally, at least one commenter requested that the Commission specifically reference provisions of the Fair Credit Reporting Act that are not modified, limited, or superceded by the G-L-B Act. Such an approach is not necessary to implement section 506 of the Act and, therefore, the final rule adopts in § 313.16 the text set out in § 313.14 of the proposal.

Section 313.17 Relation to State Laws

Section 507 of the G-L-B Act states, in essence, that Title V does not preempt any State law that provides greater protections than are provided by Title V. Determinations of whether a State law or 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 which the complaint was filed, and may be initiated by any interested party or on the Commission's own motion. The Act does not require such determinations for consistent state laws. Some commenters suggested that the Commission lacks the authority to consider preemption issues with respect to the rule, but only with respect to the Act. The Commission disagrees with the analysis. Any determination of whether a state law provides greater protection than the Act will necessarily require consideration of the rules that implement the Act.

Comments on this section ranged from those who suggested that federal law should preempt state law in every case where there is a conflict to those who encouraged the Commission to support the rights of states to enact greater protections. Some requested clarification of whether a particular state law would be considered more restrictive, while others suggested that the Commission establish in the final rule a choice of law principle for financial institutions operating in more than one state. These and other suggestions exceed the scope of this rulemaking and are better addressed, to the extent practicable, in the context of a preemption determination. Accordingly, the Commission has adopted in § 313.17 the text set out in proposed § 313.15.

Section 313.18 Effective Date; Transition Rule

Section 510 of the G-L-B Act states that, as a general rule, the relevant provisions of Title V take effect 6 months after the date on which rules are required to be prescribed, *i.e.,* November 13, 2000. However, section 510(1) authorizes the Commission to prescribe a later date in the rule enacted pursuant to section 504. The proposed rule sought comment on the effective date prescribed by the statute. It also would have required that financial institutions provide initial notices, within 30 days of the effective date of the final rule, to people who were customers as of the effective date. The preamble to the proposed rule noted that a financial institution would have to provide opt out notices before the rule's effective date if the institution wanted to continue sharing nonpublic personal information with nonaffiliated third parties without interruption.

The overwhelming majority of commenters addressing this provision requested additional time to comply with the final rule. Commenters stated that six months would not be sufficient to take the steps needed to comply with the regulation, including preparing new disclosure forms, developing software needed to track opt outs, training employees, creating management oversight systems, and undergoing internal examination and auditing to ensure compliance. Several commenters suggested that it would be less effective and potentially more confusing for consumers to receive several notices all around the end of the year 2000 than it would be for the notices to be delivered during a rolling phase-in. Others noted that the proposed effective date would place a severe strain on financial institutions at a time when other year-end notices need to be prepared and delivered. Several commenters noted that financial institutions have not budgeted for the expenses in the current year that likely will be incurred. They also noted that the disclosures regarding the standards to be followed to protect customers' records have not been proposed for comment, thereby making it impossible for financial institutions to know how to prepare at least that part of the initial privacy notices. Requests for extensions of the effective date typically ranged from 12 months to 24 months from publication of the rule.

Many commenters also stated that a 30-day phase-in for initial notices to existing customers is not feasible, given the large number of notices, the short period of time allowed, and the competing demands on financial institutions at the time when the initial notices must be sent. A few suggested that the rule require initial notices to be sent only to people who establish customer relationships after the effective date of the rule and allow a financial institution to send annual notices to existing customers at some point during the next 12 months and annually thereafter.

The Commission agrees that six months may be insufficient in certain instances for a financial institution to ensure that its forms, systems, and procedures comply with the rule. In order to accommodate situations requiring additional time, the Commission has retained the effective date of November 13, but, consistent with its authority under section 510(1) of the G-L-B Act to extend the effective date, the Commission will give financial institutions until July 1, 2001 to be in full compliance with the regulation. Financial institutions are expected, however, to begin compliance efforts promptly, to use the period prior to June 30, 2001 to implement and test their systems, and to be in full compliance by July 1, 2001. Because financial institutions will have slightly over 13 months in which to comply with the rule, there no longer is any need for a separate phase-in for providing initial notices. Thus, a financial institution will need to deliver all required opt out notices and initial notices before July 1, 2001. This extension represents a fair balance between those seeking prompt implementation of the protections afforded by the statute and those concerned about the reliability of the systems that are put in place.

Financial institutions are encouraged to provide disclosures as soon as practicable. Institutions that do not disclose nonpublic personal information to third parties have fewer burdens under the rule (both in terms of notice requirements and opt out mechanism) and should therefore be able to provide privacy notices to their consumers more expeditiously. Depending on the readiness of an institution to process opt out elections, institutions might wish to consider including the privacy and opt out notices in the same mailing as is used to provide tax information to consumers in the first quarter of 2001 so that consumers are less likely to overlook the notices.

The Commission has concluded that the extension of the date by which financial institutions must be in full compliance provides much of the relief sought by those who suggested that initial notices should not be required for existing customers. By allowing financial institutions to deliver notices over a significantly longer period of time than was proposed, the concentrated burden that would have been imposed by the proposed rule is avoided. Accordingly, the Commission

has decided not to adopt the suggestion that initial notices be required only for new customers after the effective date of the rule. Initial notices need not be given to customers whose relationships have terminated prior to the date by which institutions must be in compliance with the rule. Thus, if an account is inactive according to a financial institution's policies before July 1, 2001, then no initial notice would be required in connection with that account. However, because these former customers would remain consumers, a financial institution would have to provide a privacy and opt out notice to them if the financial institution intended to disclose their nonpublic personal information to nonaffiliated third parties beyond the exceptions in §§ 313.14 and 313.15.

The Commission notes that full compliance with the rule's restrictions on disclosures is required on July 1, 2001. To be in full compliance, institutions must have provided their existing customers with both a privacy notice and a reasonable amount of time to opt out prior to that date. If these have not been provided, the disclosure restrictions will apply. This means that a financial institution would have to cease sharing customers' nonpublic personal information with nonaffiliated third parties on that date, unless it may share the information pursuant to an exception under §§ 313.14 or 313.15. However, financial institutions that both provide the privacy notice and allow a reasonable period of time to opt out before July 1, 2001 may continue to share nonpublic personal information after that date about customers who do not opt out.

The Commission's final rule provides for an exception to the effective date to take into consideration the Board's authority to add activities that are permissible for financial holding companies to engage in. The Board's addition of permissible activities (''subsequent permissible activities'') will cause some entities that are not now financial institutions to come within the definition at a later date. The exception provides that the rule is not effective as to any entity engaging in subsequent permissible activities until the Commission so determines.

The Board has the authority to allow financial holding companies to engage in activities that are financial in nature, activities that are incidental to financial activities, and activities that are complementary to financial activities. If the Board, therefore, issues an order or regulation identifying the activity that the financial holding company may engage in without characterizing that activity, the Commission will have to determine whether any entities engaging in such activity should be covered by the privacy provisions of the G-L-B Act and, if so, to what extent. The Commission intends to publish for notice and comment its proposals with respect to entities engaging in subsequent permissible activities.

Appendix A—Sample Clauses

In order to provide additional guidance to financial institutions concerning the level of detail the Commission believe is appropriate under the statute, the Commission has set forth a variety of sample clauses for financial institutions to consider. The Commission urges financial institutions to carefully review whether these clauses accurately reflect a given institution's policies and practices before using the clauses. Financial institutions are free to use different language and to include as much additional detail as they think is appropriate in their notices.

Derivation Chart

Below is a chart showing the derivation of the sections in the final privacy rule from the proposal. Only changes are noted.

Proposal	Content of provision	Final rule
4(d)	How to provide initial notice	9(a)
N/A	New product for existing customer	4(d)
4(d)(3)	Oral delivery (privacy notice)	9(d)
4(d)(4)	Retainable notice	9(e)
N/A	Joint relationships (privacy notice)	4(f)
5(b)	How to provide annual notice	9(a) and (c)
5(c)	Terminated customer relationships	5(b)
N/A	Delivering short-form initial notices	6(d)(3)
7	Main operative provision	10
8(a)	Opt out methods; opt out notice content	7(a)
8(b)(1)	How to deliver opt out notices	9(a)
8(b)(2)	Oral delivery (opt out notice)	9(d)
8(b)(3)	Same form as initial notice	7(b)
8(b)(4)	Initial notice must accompany opt out notice	7(c)
N/A	Joint relationships (opt out notice)	7(d)
8(d)	Time to comply with opt out; continuing right to opt out	7(e) and (f)
8(e)	Duration of opt out	7(g)
8(c)(1)	Revised notices	8(a)
8(c)(2)	How to deliver revised notice	8(c)
8(c)(3)	Examples of when revised notice is required	8(b)
9	Exception for service providers and joint marketers	13
10	Exceptions for processing and servicing transactions	14
11	Other exceptions	15
12	Redisclosure and reuse	11
13	Sharing account number information	12
14	FCRA	16
15	State law	17
16	Effective date	18

Section D. Guidance for Certain Institutions

To minimize the burden and costs to a financial institution (''you'') and generally clarify the operation of the final rule, the Agencies have included this guidance that you may use in conjunction with the sample clauses in Appendix A. This guidance specifically applies to you if you:

(1) do not have any affiliates;

(2) only disclose nonpublic personal information to nonaffiliated third

parties in accordance with an exception under §§ 313.14 or 313.15, such as in connection with servicing or processing a financial product or service that a consumer requests or authorizes ; and

(3) do not reserve the right to disclose nonpublic personal information to nonaffiliated third parties, except under §§ 313.14 and 313.15.[39]

In addition, if you disclose nonpublic personal information in accordance with the exception in § 313.13 for service providers and joint marketers, you also must include an accurate description of that information, as illustrated by the sample clause in section *(K)* below.

In general, if you disclose nonpublic personal information to nonaffiliated third parties only as authorized under an exception, then your only responsibilities under the regulation are to provide initial and annual notices to each of your customers. You do not need to provide an opt out notice or opt out rights to your customers.

A. Initial notice to customers. You must provide an initial notice to each of your customers. A customer is a natural person who has a continuing relationship with you, as described in § 313.4(c). For instance, a ''pay day'' lender who extends a loan to an individual has a customer relationship with that individual. By contrast, if the ''pay day'' lender only cashes a check for that individual, there is no customer relationship; even if that individual repeatedly cashes checks with the same pay-day lender, she remains only the lender's consumer. In other words, you must provide initial and annual notices to each of your customers, but not to others.

B. Time to provide initial notice. You must provide an initial privacy notice to each of your customers not later than when you establish a customer relationship (§ 313.4(a)(1)). For instance, you must provide a privacy notice to an individual not later than when that individual executes the contract to open a checking account. Thus, you can provide the notice to a checking account customer together with the account agreement and signature card.

Similarly, in the case of extending a mortgage loan, you must provide a privacy notice to an individual not later than when you and the individual enter into an agreement that you will serve as the mortgage lender. For example, you can provide the notice to an individual together with the documents (or other forms) that constitute the contract to extend the loan. You may always deliver your privacy notices earlier than required.

If one of your existing customers obtains a new financial product or service from you, then you need not provide another initial notice to that customer (§ 313.4(d)) if that earlier notice covered the subsequent product.

For instance, if Alison Individual enters Lender's offices for the first time on July 2, 2001 to obtain a mortgage, then Lender complies with § 313.4(a)(1) of the rule if it provides an initial notice to Alison with the mortgage agreement. When Alison obtains her mortgage, she becomes a customer of Lender. Alison makes regular payments to Lender on her mortgage and, two years later, returns to Lender to obtain a credit card. If the initial notice that Lender provided to Alison is accurate with respect to the terms of that credit card, then Lender need not provide another initial notice to her when she obtains the credit card because Lender has already provided a notice to Alison that covers that relationship.

C. Method of providing the initial notice. You must provide your initial notice so that each customer can reasonably be expected to receive actual notice of it, in writing (§ 313.9(a)). For example, you may provide the initial notice by mailing a printed copy of it together with a loan contract. Similarly, you may provide the initial notice by hand-delivering a printed copy of it to the customer together with a deposit account agreement.

D. Compliance with initial notice requirement for existing customers by effective date. You must provide an initial notice to each of your current customers not later than July 1, 2001 (§ 313.18(b)). You may do so by mailing a printed copy of the notice to the customer's last known address.

E. Annual notice. During the continuation of the customer relationship, you must provide an annual notice to the customer, as described in § 313.5(a). You must provide an annual notice to each customer at least once in any period of 12 consecutive months during which the customer relationship exists. You may define the 12-consecutive-month period, but must consistently apply that period to the customer. You may define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice.

For example, assume that Lender defines the 12-consecutive-month period as a calendar year and provides annual notices to all of its customers on October 1 of each year. If Alison Individual obtained her mortgage with Lender on July 2, 2001, thereby becoming a customer, then Lender must provide an initial notice to Alison together with the mortgage agreement or earlier. Lender must provide an annual notice to Alison by December 31, 2002. If Lender provides an annual notice to Alison on October 1, 2002, as it does for other customers, then it must provide the next annual notice to Alison not later than October 1, 2003.

F. Method of providing the annual notice. Like the initial notice, you must provide the annual notice so that each customer can reasonably be expected to receive actual notice of it, in writing (§ 313.9(a)). You may do so by mailing a printed copy of the notice to the customer's last known address.

G. Joint accounts. If two or more customers jointly obtain a financial product or service, then you may provide one initial notice to those customers jointly. Similarly, you may provide one annual notice to those customers jointly (§ 313.4(f)).

H. Information described in the initial and annual notices. The initial and annual notices must include an accurate description of the following four items of information:

(a) The categories of nonpublic personal information that you collect (§ 313.6(a)(1));

(b) The fact that you do not disclose nonpublic personal information about your current customers to affiliates or nonaffiliated third parties, except as authorized by §§ 313.14 and 313.15 (§ 313.6(a)(2)–(3), (9)). When describing the categories with respect to those parties, you are required to state only that you make disclosures to other nonaffiliated third parties as permitted by law (§ 313.6(b));

(c) 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 (§ 313.6(a)(4));

(d) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (§ 313.6(a)(8)).

For each of these four items of information above, you may use a sample clause from Appendix A. The Agencies emphasize that you may use a sample clause only if that clause

[39] If you disclose or reserve the right to disclose nonpublic personal information to a nonaffiliated third party under other circumstances, you must comply with other provisions in the rule, notably §§ 313.7, 313.8, and 313.13, if applicable. If you disclose or reserve the right to disclose nonpublic personal information to an affiliate you must comply with other provisions in the rule, notably § 313.6(a)(7), as applicable.

accurately describes your actual policies and practices.

I. Example of notice. A financial institution (''Lender'') that (i) does not have any affiliates and (ii) only discloses nonpublic personal information to nonaffiliated third parties as authorized under §§ 313.14 and 313.15, may comply with the requirements of § 313.6 of the rule by using the following notice, if applicable.

Lender collects nonpublic personal information about you from the following sources:

- *Information we receive from you on applications or other forms;*
- *Information about your transactions with us or others; and*
- *Information we receive from a consumer reporting agency.*[40]

We do not disclose any nonpublic personal information about you to anyone, except as permitted by law.

If you decide to pay off your loan(s), we will adhere to the privacy policies and practices as described in this notice.

Lender restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. Lender maintains physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

J. Initial and annual notices must be clear and conspicuous. The Commission emphasizes that you must ensure that both the initial and annual notices are clear and conspicuous, as defined in § 313.3(b).

K. Example of notice for disclosure to service providers and joint marketers. If you disclose nonpublic personal information in accordance with the exception in § 313.13, for service providers and joint marketers, you also must include an accurate description of that information. You may comply with the requirements of § 313.13 of the rule by including the following sample clause, if applicable, in the example of notice described in section (*I*) above:

We may disclose all of the information we collect, as described [describe location in the notice, such as ''above'' or ''below'], to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

[40] You only need to describe those general categories that apply to your policies and practices. Accordingly, if you do not collect information from ''a consumer reporting agency,'' for instance, then you need not describe that category in your notices.

Section E. Final Regulatory Flexibility Analysis

The Regulatory Flexibility Act (5 U.S.C. 601–612) (''RFA'') requires, subject to certain exceptions, that federal agencies prepare an initial regulatory flexibility analysis (''IRFA'') with a proposed Rule and a final regulatory flexibility analysis (''FRFA'') with a final Rule, unless the agency certifies that the Rule will not have a significant economic impact on a substantial number of small entities. At the time the proposed Rule was issued, the Commission believed that the G-L-B Act's requirements accounted for most, if not all, of the economic impact of the Rule, but decided to publish the IRFA to ensure that in developing the final Rule it adequately considered the impact on small businesses. After reviewing the comments submitted in response to the proposed Rule, the Commission continues to believe that the burden imposed on small institutions stems primarily from the statute and that certification would be proper. However, in order to assist those entities with comprehending and complying with the final Rule, the Commission has determined that it is appropriate to publish a FRFA analyzing the Rule as a whole and highlighting provisions that will particularly accommodate the needs of small businesses.

This FRFA incorporates the Commissions's initial findings, as set forth in the IRFA; addresses the comments submitted in response to the IRFA; and describes the steps the Commission has taken in the final Rule to minimize the impact on small entities, consistent with the objectives of the G-L-B Act. The Commission is publishing with this part a guide for entities that do not share any nonpublic personal information, a disproportionate number of which are likely to be small businesses. (See Supplementary Information, Section C.) Also, in accordance with Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104–121), the Commission will in the near future issue a compliance guide to assist small entities in complying with this rule.

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

The final Rule implements the provisions of Title V, Subtitle A of the G-L-B Act, which addresses consumer privacy. In general, these statutory provisions require financial institutions to provide notice to consumers about the institution's privacy policies and practices, describe the conditions under which financial institutions may disclose nonpublic personal information about consumers to nonaffiliated third parties, and permit consumers to prevent institutions from sharing nonpublic personal information about them with certain non-affiliated third parties by ''opting out'' of that disclosure.

Section 504 of the G-L-B Act requires the Commission to prescribe ''such regulations as may be necessary'' to carry out the purposes of Title V, Subtitle A. In the absence of these regulations, the substantive burdens imposed by the Act (*e.g.,* the notice, information-sharing restrictions, and opt-out requirements) would have become effective and binding upon financial institutions within one year of the enactment of the law. The Commission believes that the final Rule gives the private sector greater certainty and flexibility with respect to compliance with the statute, as well as clearer guidance as to how the Commission will enforce it.

Description and Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

Determining a precise estimate of the number of small entities that are financial institutions within the meaning of the proposed Rule is not readily feasible. The definition of ''financial institution'' includes any institution the business of which is engaging in a financial activity, as described in section 4(k) of the Bank Holding Company Act, which incorporates by reference the activities listed in 12 CFR 225.28 and 12 CFR 211.5(d). These include lenders, loan brokers and servicers, collection agencies, financial advisors, tax preparers, real estate settlement services, property appraisers, and others. The G-L-B Act does not identify for purposes of the Commission's jurisdiction any specific category of financial institution; section 505(a)(7) vests the Commission with enforcement authority with respect to ''any other financial institution or other person that is not subject to the jurisdiction of any [other] agency or authority [charged with enforcing the statute].'' Jurisdiction is assigned to other agencies with respect to banks, bank holding companies, and their subsidiaries and affiliates; savings associations, federal credit unions, and their subsidiaries; securities brokers and dealers; investment advisers and investment companies; and insurers.

Although the Commission requested comment on these issues, it did not receive a response sufficient to provide a basis for determining the number of small entities subject to the final Rule. In the absence of such information, there is no way to estimate precisely the number of affected entities that share nonpublic personal information with nonaffiliated third parties or that establish customer relationships with consumers and therefore assume greater disclosure obligations.

Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

The Commission incorporates by reference its description of the projected reporting, recordkeeping, and other compliance requirements of the Rule, as set forth in the IRFA. The Commission has not received any comments that necessitate modification of its previous description of projected compliance requirements. Based on the information the Commission submitted to the Office of Management and Budget, which included an estimated average annual burden over the three-year period of clearance of 4.03 million hours and $87.3 million, OMB has approved the final Rule for the related purposes of the Paperwork Reduction Act. (See section F, infra.)

Among the principal obligations that Title V, Subtitle A of the G-L-B Act, as executed by the final Rule, imposes upon financial institutions is the preparation of notices explaining their privacy policies and practices. Institutions are required to provide those notices to consumers as specified in the Rule, and institutions that disclose nonpublic personal information about their consumers to nonaffiliated third parties will be required to provide opt out notices, as well as a reasonable opportunity to opt out of certain disclosures, to their consumers. These institutions will have to develop systems for keeping track of consumers' opt out directions. Some institutions, particularly those that disclose nonpublic information about consumers to nonaffiliated third parties, will likely need the advice of legal counsel to ensure that they comply with the Rule and may also require computer programming changes and additional staff training.

A detailed, section-by-section analysis of the final Rule is set forth above in section B. of the Supplementary Information part of this notice.

Summary of Significant Issues Raised by Public Comments and Description of Steps the Commission Has Taken To Minimize the Significant Economic Impact on Small Entities

The Commission has sought to minimize the burden on all businesses, including small entities, in promulgating this final rule. Although one method of accomplishing this objective would be to adopt a specific exemption for small entities, the G-L-B Act does not authorize the Commission to create exemptions based on an institution's size. Further, the Commission believes that different compliance standards would be inconsistent with the purpose of Title V, which is to offer all consumers some measure of control over the dissemination of the nonpublic personal information that they provide to financial institutions, regardless of the institution's size. As section 501(a) of the Act declares, ''[i]t is the policy of the Congress that *each* financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.'' (Emphasis added).

Notwithstanding its limited authority to accommodate the specific needs of smaller institutions, the Commission has requested and analyzed throughout this rulemaking process information regarding the economic impact of the G-L-B Act's requirements for all financial institutions, including small entities. The proposed rule and the IRFA included a number of questions for public comment regarding the costs associated with complying with the Rule and the impact on small entities. Although the Commission received few comments that specifically addressed the regulatory flexibility analysis, it carefully considered comments concerning the substantive provisions of the Rule.[41] The discussion below reviews some of those key recommendations and corresponding changes adopted in the final Rule that accommodate those suggestions. Many of the steps taken by the Commission will benefit all institutions, regardless of size, while others will especially reduce the regulatory burden for small entities. For a more complete discussion of these changes, see the section-by-section analysis under section C of the Supplementary Information part of this notice.

Effective Date

Subject to section 510 of the G-L-B Act, the relevant provisions of Title V take effect on November 13, 2000. However, section 510(1) authorizes the Commission to prescribe a later date in the regulations enacted pursuant to section 504. The proposed Rule sought comment on the effective date prescribed by the statute. The overwhelming majority of commenters requested additional time to comply with the final rule. Several commenters noted that financial institutions may encounter difficulty managing the expenses and resources required to comply with the final rule as the institution's budget for the current year was established prior to the issuance of the proposed regulation. This may be especially true for small institutions that face already tight budgetary constraints due to heightened competition. In response to these concerns, the Commission has retained the effective date of November 13, 2000 but, consistent with its authority under section 510(1) of the statute, will give financial institutions until July 1, 2001 to be in full compliance with the final Rule. This additional time should reduce compliance costs for institutions by allowing additional time to budget for any necessary expenses and to implement all necessary operational changes required to comply with this Rule.

Examples

Throughout the final Rule, the Commission has included examples of conduct that illustrate ways to comply with particular provisions. As the section-by-section analysis above and the Rule itself explain, these examples are not exclusive, but they should lessen for institutions the burdens imposed by the Rule by clarifying that compliance with an applicable example constitutes compliance with the applicable provision.

Definition of Nonpublic Personal Information

In the proposed rule, the Commission provided two alternatives for defining nonpublic personal information. The

[41] Even if the Commission had the authority to craft exceptions strictly based on the size of institutions, the comments received did not provide the amount, specificity, or consistency of information required to make such targeted policy determinations. For example, the Commission received one comment from a regional department store retailer with an estimated annual volume of $700 million in 1999. This small retail chain stated that approximate mailing costs associated with issuing privacy notices would be $400,000–$500,000, or 4%–5% of its net income. Another commenter estimated that total compliance costs would total $97,400 for an institution with assets of approximately $100 million. Based on these widely disparate projections and scant statistics, an exception applicable to all ''small entities'' would be impracticable and inappropriate.

first, (Alternative A) deemed information as publicly available only if a financial institution *actually obtained* the information from a public source, whereas the second (Alternative B) treated information as publicly available if a financial institution *could* obtain it from such a source. A vast majority of commenters favored Alternative B as significantly less burdensome than Alternative A. In response to these comments, the final Rule adopts a modified version of Alternative B, which is more fully explained in the section-by-section analysis.

Content of Notices

Many commenters interpreted the proposed Rule as mandating lengthy, confusing privacy notices that would offer little benefit to consumers, and asked for clarification with respect to the content of those disclosures. Although the Commission believes that the notice obligations are not unduly burdensome, in the final Rule it has taken a number of steps to clarify the requirements imposed by the G-L-B Act. The final Rule substantially revises the examples of disclosures that would satisfy the Rule, includes sample clauses that might be used, and adds a new provision for ''short-form'' privacy notices to a consumer that does not become a customer, provided the institution gives the consumer an opt out notice and a reasonably convenient method of obtaining a copy of the full privacy notice. It also retains the simplified notice provision for institutions that do not share nonpublic personal information with nonaffiliated third parties, except pursuant to the exceptions set forth in §§ 313.14 and 313.15 of this part. These measures may be particularly helpful to smaller institutions who do not disclose nonpublic personal information except under those and other exceptions in the final Rule.

In addition, the Commission has included with the final Rule sample disclosures that institutions may use to draft their privacy and opt out notices required by this part. As discussed in the section-by-section analysis above, these clauses are provided to convey to institutions the requisite level of detail that these notices must contain. Institutions can also consult the Guide for Certain Financial Institutions (''Guide''). The Guide generally clarifies the operation of the final Rule. It also provides an example of a notice for institutions, including small entities, that only share nonpublic personal information with nonaffiliated third parties pursuant to the exceptions provided in §§ 313.14 and 313.15. The Guide may be used in conjunction with the sample clauses contained in Appendix A. Like the examples discussed above, the sample disclosures and the Guide are intended to minimize the burden of complying with the final Rule, by reducing, among other costs, the need for legal advice.

Joint Account Holders

Another frequent comment addressed the provision of notice to and effect of opt outs exercised by joint account holders. As the section-by-section analysis describes, the final Rule clarifies that institutions may provide a single notice to joint account holders (unless otherwise requested), with the understanding that a decision to opt out made by one of the joint account holders will, absent a provision to the contrary in the opt out notice, be effective with respect to each of the account holders. By reducing the number of notices that institutions are required to provide, this flexibility will particularly benefit those institutions, including small entities, that do not share nonpublic personal information with nonaffiliated third parties, except pursuant to an exception.

New Notices Not Required for Each New Financial Product or Service

Some commenters expressed concern that the proposed rule may require a new initial notice each time a consumer obtains a new financial product or service. This would be especially burdensome for an institution that adopts a universal privacy policy that covers multiple products and services. To address these concerns and minimize economic burden, the final Rule was clarified to instruct institutions that a new initial notice is not required if the institution has given the customer the institution's initial notice, and that notice remains accurate with respect to the new product or service.

Section F. Paperwork Reduction Act

Pursuant to the Paperwork Reduction Act, as amended, 44 U.S.C. 3501 *et seq.*, the Commission submitted the proposed Rule to the Office of Management and Budget (OMB) for review. The OMB has approved the Rule's information collection requirements.[42] A **Federal Register** notice with a 30-day comment period of soliciting comments on this collection of information was published on March 1, 2000 (65 FR 11174). The Commission did not receive any comments that necessitated modifying its original burden estimates for the Rule's notice requirements.

[42] The assigned OMB clearance number is 3084–0121.

Section G. Final Rule

List of Subjects in 16 CFR Part 313

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

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

PART 313—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.
313.1 Purpose and scope.
313.2 Rule of construction.
313.3 Definitions.

Subpart A—Privacy and Opt Out Notices

313.4 Initial privacy notice to consumers required.
313.5 Annual privacy notice to customers required.
313.6 Information to be included in privacy notices.
313.7 Form of opt out notice to consumers; opt out methods.
313.8 Revised privacy notices.
313.9 Delivering privacy and opt out notices.

Subpart B—Limits on Disclosures

313.10 Limitation on disclosure of nonpublic personal information to nonaffiliated third parties.
313.11 Limits on redisclosure and reuse of information.
313.12 Limits on sharing account number information for marketing purposes.

Subpart C–Exceptions

313.13 Exception to opt out requirements for service providers and joint marketing.
313.14 Exceptions to notice and opt out requirements for processing and servicing transactions.
313.15 Other exceptions to notice and opt out requirements.

Subpart D—Relation to Other Laws; Effective Date

313.16 Protection of Fair Credit Reporting Act.
313.17 Relation to State laws.
313.18 Effective date; transition rule.

Appendix A to Part 313—Sample Clauses

Authority: 15 U.S.C. 6801 *et seq.*

§ 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 customers 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 §§ 313.13, 313.14, and 313.15.

(b) *Scope.* This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural 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 its business is engaging in a financial activity as 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, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission. 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. Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d–1320d–8. Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

§ 313.2 Rule of construction.

The examples in this part and the sample clauses in Appendix A of this part are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this part. For non-federally insured credit unions, compliance with an example or use of a sample clause contained in 12 CFR part 716, to the extent applicable, constitutes compliance with this part. For intrastate securities broker-dealers and investment advisors not registered with the Securities and Exchange Commission, compliance with an example or use of a sample clause contained in 17 CFR part 248, 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 in the notice.

(2) *Examples*—(i) *Reasonably understandable.* You make your notice reasonably understandable if you:

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

(B) Use short explanatory sentences or 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 whenever possible; and

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

(ii) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if 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;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

(iii) *Notices on web sites.* If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(c) *Collect* means to obtain information that you organize or can retrieve by the name of an individual or by identifying number, symbol, or other identifying particular assigned to the individual, 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, or 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.

(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, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(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) *Continuing relationship*. A consumer has a continuing relationship with you if the consumer:

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

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(E) 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;

(F) Enters into a lease of personal property on a non-operating basis 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;

(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 financial institution or department of any company);

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(K) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) *No continuing relationship*. A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a 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;

(C) You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(j) *Federal functional 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; and

(6) The Securities and Exchange Commission.

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

(2) *Examples of financial institution*.

(i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(iii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines,

is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act.

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 211.5(d)(15) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act.

(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 §§ 313.14 and 313.15 of this part.

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities.

(4) *Examples of entities that are not significantly engaged in financial activities.* (i) A retailer is not a financial institution if its only means of extending credit are occasional ''lay away'' and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to ''run a tab.''

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

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

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

(m)(1) *Nonaffiliated third party* means any person except:

(i) Your affiliate; or

(ii) 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).

(2) *Nonaffiliated third party* includes any company that is an affiliate by virtue of your or your affiliate's direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

(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 that is not publicly available.

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

(i) Publicly available information, except as included on a list described 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 that is not publicly available.

(3) *Examples of lists*—(i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

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

(i) A consumer provides 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) *Information included.* Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(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;

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

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet ''cookie'' (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) *Information not included.* 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; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(p)(1) *Publicly available information* means any information that you have a reasonable basis to believe 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) *Reasonable basis.* You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) *Examples*—(i) *Government records.* Publicly available information in government records includes information 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 a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) *Reasonable basis*—(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(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 Gramm-Leach-Bliley Act.

Subpart A—Privacy and Opt Out Notices

§ 313.4 Initial privacy notice to consumers required.

(a) *Initial notice requirement.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:

(1) *Customer.* An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before 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 §§ 313.14 and 313.15.

(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) of this section if:

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 313.14 and 313.15; 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 when you and the consumer enter into a continuing relationship.

(2) *Special rule for loans.* You establish a customer relationship with a consumer when you originate a loan to the consumer for personal, family, or household purposes. If you subsequently transfer the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3)(i) *Examples of establishing customer relationship.* You establish a customer relationship when the consumer:

(A) Opens a credit card account with you;

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

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

(D) 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);

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

(F) Executes the lease for personal property with you;

(G) Is an obligor on an account that you purchased from another financial institution and whom you have located and begun attempting to collect amounts owed on the account; or

(H) Provides you with the information necessary for you to compile and provide access to all of the consumer's on-line financial accounts at your Web site.

(ii) *Examples of loan rule.* You establish a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when you:

(A) Originate the loan to the consumer and retain the servicing rights; or

(B) Purchase the servicing rights to the consumer's loan.

(d) *Existing customers.* When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family, or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:

(1) You may provide a revised privacy notice, under § 313.8, that covers the customer's new financial product or service; or

(2) If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

(e) *Exceptions to allow subsequent delivery of notice.* (1) 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) Establishing the customer relationship is not at the customer's election; or

(ii) Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.

(2) *Examples of exceptions*—(i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if you acquire a customer's loan, or the servicing rights, from another financial institution and the customer does not have a choice about your acquisition.

(ii) *Substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction when:

(A) You and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service; or

(B) You establish a customer relationship with an individual under a program authorized by Title IV of the Higher Education Act of 1965 (20 U.S.C. 1070 *et seq.*) or similar student loan programs where loan proceeds are disbursed promptly without prior communication between you and the customer.

(iii) *No substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at your office or through other means by which the customer may view the notice, such as through a web site.

(f) *Delivery.* When you are required to deliver an initial privacy notice by this section, you must deliver it according to § 313.9. If you use a short-form initial notice for non-customers according to § 313.6(d), you may deliver your privacy notice according to § 313.6(d)(3).

§ 313.5 Annual privacy notice to customers required.

(a)(1) *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 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

(2) *Example.* You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

(b)(1) *Termination of customer relationship.* You are not required to provide an annual notice to a former customer.

(2) *Examples.* Your customer becomes a former customer when:

(i) In the case of a closed-end loan, the customer 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 sell the receivables without retaining servicing rights;

(iii) In the case of credit counseling services, the customer has failed to make required payments under a debt management plan, has been notified that the plan is terminated, and you no longer provide any statements or notices to the customer concerning that relationship;

(iv) In the case of mortgage or vehicle loan brokering services, your customer has obtained a loan through you (and you no longer provide any statements or notices to the customer concerning that relationship), or has ceased using your services for such purposes;

(v) In the case of tax preparation services, you have provided and received payment for the service and no longer provide any statements or notices to the customer concerning that relationship;

(vi) In the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, you have received payment, or you have completed all of your responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.

(vii) In cases where there is no definitive time at which the customer relationship has terminated, you have not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material.

(c) *Special rule for loans.* If you do not have a customer relationship with a consumer under the special rule for loans in § 313.4(c)(2), then you need not provide an annual notice to that consumer under this section.

(d) *Delivery.* When you are required to deliver an annual privacy notice by this section, you must deliver it according to § 313.9.

§ 313.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under §§ 313.4, 313.5, and 313.8 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§ 313.14 and 313.15;

(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 §§ 313.14 and 313.15;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 313.13 (and no exception under §§ 313.14 or 313.15 applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the consumer's right under § 313.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

(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);

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

(9) Any disclosure that you make under paragraph (b) of this section.

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information to third parties as authorized under §§ 313.14 and 313.15, 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 required to state only that you make disclosures to other

nonaffiliated third parties as permitted by law.

(c) *Examples*—(1) *Categories of nonpublic personal information that you collect.* You satisfy the requirement to categorize the nonpublic personal information that you collect if you list the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with you or your affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer reporting agency.

(2) *Categories of nonpublic personal information you disclose*—(i) You satisfy the requirement to categorize the nonpublic personal information that you disclose if you list the categories described in paragraph (e)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.

(ii) If you reserve the right to disclose all of the nonpublic personal information about consumers that you collect, you may simply state that fact without describing the categories or examples of the nonpublic personal information you disclose.

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.* You satisfy the requirement to categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information if you list them using the following categories, as applicable, and a few applicable examples to illustrate the significant types of third parties covered in each category.

(i) Financial service providers, followed by illustrative examples such as mortgage bankers, securities broker-dealers, and insurance agents.

(ii) Non-financial companies, followed by illustrative examples such as retailers, magazine publishers, airlines, and direct marketers; and

(iii) Others, followed by examples such as nonprofit organizations.

(4) *Disclosures under exception for service providers and joint marketers.* If you disclose nonpublic personal information under the exception in § 313.13 to a nonaffiliated third party to market products or services that you offer alone or jointly with another financial institution, you satisfy the disclosure requirement of paragraph (a)(5) of this section if you:

(i) List the categories of nonpublic personal information you disclose, using the same categories and examples you used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) State whether the third party is:

(A) A service provider that performs marketing services on your behalf or on behalf of you and another financial institution; or

(B) A financial institution with whom you have a joint marketing agreement.

(5) *Simplified notices.* If you do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under §§ 313.14 and 313.15, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

(6) *Confidentiality and security.* You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if you do both of the following:

(i) Describe in general terms who is authorized to have access to the information; and

(ii) State whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use.

(d) *Short-form initial notice with opt out notice for non-customers*—(1) You may satisfy the initial notice requirements in §§ 313.4(a)(2), 313.7(b), and 313.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in § 313.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that your privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain that notice.

(3) You must deliver your short-form initial notice according to § 313.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to § 313.9.

(4) *Examples of obtaining privacy notice.* You provide a reasonable means by which a consumer may obtain a copy of your privacy notice if you:

(i) Provide a toll-free telephone number that the consumer may call to request the notice; or

(ii) For a consumer who conducts business in person at your office, maintain copies of the notice on hand that you provide to the consumer immediately upon request.

(e) *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.

(f) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this part.

§ 313.7 Form of opt out notice to consumers; opt out methods.

(a) (1) *Form of opt out notice.* If you are required to provide an opt out notice under § 313.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. 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) *Adequate opt out notice.* You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you:

(A) Identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose, and all of the categories of nonaffiliated third parties to which you disclose the information, as described in § 313.6(a) (2) and (3) and state that the consumer can opt out of the disclosure of that information; and

(B) Identify the financial products or services that the consumer obtains from you, either singly or jointly, to which the opt out direction would apply.

(ii) *Reasonable opt out means.* 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;

(B) Include a reply form that includes the address to which the form should be mailed; or

(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) Provide a toll-free telephone number that consumers may call to opt out.

(iii) *Unreasonable opt out means.* You *do not* provide a reasonable means of opting out if:

(A) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(B) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that you provided with the initial notice but did not include with the subsequent notice.

(iv) *Specific opt out means.* You may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

(b) *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.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice later than required for the initial notice in accordance with § 313.4, you must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

(d) *Joint relationships*—(1) If two or more consumers jointly obtain a financial product or service from you, you may provide a single opt out notice, unless one or more of those consumers requests a separate opt out notice. Your opt out notice must explain how you will treat an opt out direction by a joint consumer (as explained in paragraph (d)(5)(ii)of this section).

(2) Any of the joint consumers may exercise the right to opt out. You may either:

(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(ii) Permit each joint consumer to opt out separately.

(3) If you permit each joint consumer to opt out separately, you must permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) You may not require *all* joint consumers to opt out before you implement *any* opt out direction.

(5) *Example.* If John and Mary have a joint credit card account with you and arrange for you to send statements to John's address, you may do any of the following, but you must explain in your opt out notice which opt out policy you will follow:

(i) Send a single opt out notice to John's address, but you must accept an opt out direction from either John or Mary.

(ii) Treat an opt out direction by either John or Mary as applying to the entire account. If you do so, and John opts out, you may not require Mary to opt out as well before implementing John's opt out direction.

(iii) Permit John and Mary to make different opt out directions. If you do so,

(A) You must permit John and Mary to opt out for each other;

(B) If both opt out, you must permit both to notify you in a single response (such as on a form or through a telephone call); and

(C) If John opts out and Mary does not, you may only disclose nonpublic personal information about Mary, but not about John and not about John and Mary jointly.

(e) *Time to comply with opt out.* You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive it.

(f) *Continuing right to opt out.* A consumer may exercise the right to opt out at any time.

(g) *Duration of consumer's opt out direction*—(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that you collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with you, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) *Delivery.* When you are required to deliver an opt out notice by this section, you must deliver it according to § 313.9.

§ 313.8 Revised privacy notices.

(a) *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 that consumer under § 313.4, unless:

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

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

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

(4) the consumer does not opt out.

(b) *Examples*—(1) Except as otherwise permitted by §§ 313.13, 313.14, and 313.15, you must provide a revised notice before you:

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

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

(iii) Disclose nonpublic personal information about a former customer to a nonaffiliated third party if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.

(2) A revised notice is not required if you disclose nonpublic personal information to a new nonaffiliated third party that you adequately described in your prior notice.

(c) *Delivery.* When you are required to deliver a revised privacy notice by this section, you must deliver it according to § 313.9.

§ 313.9 Delivering privacy and opt out notices.

(a) *How to provide notices.* You must provide any privacy notices and opt out notices, including short-form initial notices, that this part requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

(b)(1) *Examples of reasonable expectation of actual notice.* You may reasonably expect that a consumer will receive actual notice if you:

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

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

(iii) For the consumer who conducts transactions electronically, clearly and conspicuously 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;

(iv) 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.

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

(i) Only post a sign in your branch or office or generally publish

advertisements of your privacy policies and practices;

(ii) Send the notice via electronic mail to a consumer who does not obtain a financial product or service from you electronically.

(c) *Annual notices only.* You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:

(1) The customer uses your web site to access financial products and services electronically and agrees to receive notices at the web site and you post your current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.

(d) *Oral description of notice insufficient.* You may not provide any notice required by this part solely by orally explaining the notice, either in person or over the telephone.

(e) *Retention or accessibility of notices for customers*—(1) For customers only, you must provide the initial notice required by § 313.4(a)(1), the annual notice required by § 313.5(a), and the revised notice required by § 313.8 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) *Examples of retention or accessibility.* You provide a privacy notice to the customer so that the customer can retain it or obtain it later if you:

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

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

(iii) Make your current privacy notice available on a web site (or a link to another web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the web site.

(f) *Joint notice with other financial institutions.* You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions.

(g) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from you, you may satisfy the initial, annual, and revised notice requirements of §§ 313.4(a), 313.5(a), and 313.8(a) by providing one notice to those consumers jointly, unless one or more of those consumers requests separate notices.

Subpart B—Limits on Disclosures

§ 313.10 Limits on disclosure of nonpublic personal information 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 § 313.7;

(iii) You have given the consumer a reasonable opportunity, before 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 §§ 313.13, 313.14, and 313.15.

(3) *Examples of reasonable opportunity to opt out.* You provide a consumer with a reasonable opportunity to opt out if:

(i) *By mail.* You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days from the date you mailed the notices.

(ii) *By electronic means.* A customer opens an on-line account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(iii) *Isolated transaction with consumer.* For an isolated transaction, such as the purchase of a money order by a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section 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) You must comply with this section, 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.

§ 313.11 Limits on redisclosure and reuse of information.

(a)(1) *Information you receive under an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in § 313.14 or 313.15 of this part, your disclosure and use of that information is limited as follows:

(i) You may disclose the information to the affiliates of the financial institution from which you received the information;

(ii) You may disclose the information to your affiliates, but your affiliates may, in turn, disclose and use the information only to the extent that you may disclose and use the information; and

(iii) You may disclose and use the information pursuant to an exception in § 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.

(2) *Example.* If you receive a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in § 313.14(a), you may disclose that information under any exception in § 313.14 or 313.15 in the ordinary course of business in order to provide those services. You could also disclose that information in response to a properly authorized subpoena. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

(b)(1) *Information you receive outside of an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution other than under an exception in § 313.14 or 313.15 of this part, you may disclose the information only:

(i) To the affiliates of the financial institution from which you received the information;

(ii) To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and

(iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.

(2) *Example.* If you obtain a customer list from a nonaffiliated financial institution outside of the exceptions in § 313.14 and 313.15:

(i) You may use that list for your own purposes; and

(ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed the list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list, as limited by the opt out direction of each consumer whose nonpublic personal information you intend to disclose, and you may disclose the list in accordance with an exception in § 313.14 or 313.15, such as to your attorneys or accountants.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal information to a nonaffiliated third party under an exception in § 313.14 or 313.15 of this part, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to your affiliates;

(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and

(3) The third party may disclose and use the information pursuant to an exception in § 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) *Information you disclose outside of an exception.* If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in § 313.14 or 313.15 of this part, the third party may disclose the information only:

(1) To your affiliates;

(2) To its affiliates, but its affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if you made it directly to that person.

§ 313.12 Limits on sharing account number information for marketing purposes.

(a) *General prohibition on disclosure of account numbers.* 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 consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(b) *Exceptions.* Paragraph (a) of this section does not apply if you disclose an account number or similar form of access number or access code:

(1) To your agent or service provider solely in order to perform marketing for your own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account; or

(2) To a participant in a private label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

(c) *Examples*—(1) *Account number.* An account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code.

(2) *Transaction account.* A transaction account is an account other than a deposit account or a credit card account. A transaction account does not include an account to which third parties cannot initiate charges.

Subpart C—Exceptions

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

(a) *General rule.* (1) The opt out requirements in §§ 313.7 and 313.10 do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

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

(ii) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out those purposes.

(2) *Example.* If you disclose nonpublic personal information under this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out that joint marketing.

(b) *Service may include joint marketing.* The services a nonaffiliated third party performs for you 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.

§ 313.14 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), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing a financial product or service that a consumer requests or authorizes;

(2) Maintaining or servicing 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

(3) 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:

(A) The authorization, settlement, 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.

§ 313.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 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 a federal functional regulator, 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), a State insurance authority, with respect to any person domiciled in that insurance authority's State that is engaged in providing insurance, and the Federal Trade Commission), 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 § 313.7(f).

Subpart D—Relation to Other Laws; Effective Date

§ 313.16 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.

§ 313.17 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 federal functional regulator or other authority.

§ 313.18 Effective date; transition rule.

(a) *Effective date.* (1) *General rule.* This part is effective November 13, 2000. In order to provide sufficient time for you to establish policies and systems to comply with the requirements of this part, the Commission has extended the time for compliance with this part until July 1, 2001.

(2) *Exception.* This part is not effective as to any institution that is significantly engaged in activities that the Federal Reserve Board determines, after November 12, 1999, (pursuant to its authority in Section 4(k)(1–3) of the Bank Holding Company Act), are activities that a financial holding company may engage in, until the Commission so determines.

(b)(1) *Notice requirement for consumers who are your customers on the compliance date.* By July 1, 2001, you must have provided an initial notice, as required by § 313.4, to consumers who are your customers on July 1, 2001.

(2) *Example.* You provide an initial notice to consumers who are your customers on July 1, 2001, if, by that

date, you have established a system for providing an initial notice to all new customers and have mailed the initial notice to all your existing customers.

(c) *Two-year grandfathering of service agreements.* Until July 1, 2002, a contract that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 313.13(a)(1) of this part, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as you entered into the contract on or before July 1, 2000.

Appendix A to Part 313—Sample Clauses

Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets and income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A–1—Categories of Information You Collect (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(1) to describe the categories of nonpublic personal information you collect.

Sample Clause A–1

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates, or others; and
- Information we receive from a consumer reporting agency.

A–2—Categories of Information You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use one of these clauses, as applicable, to meet the requirement of § 313.6(a)(2) to describe the categories of nonpublic personal information you disclose. You may use these clauses if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–2, Alternative 1

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–2, Alternative 2

We may disclose all of the information that we collect, as described [*describe location in the notice, such as ''above'' or ''below''*].

A–3—Categories of Information You Disclose and Parties to Whom You Disclose (Institutions That Do Not Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirements of §§ 313.6(a)(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose. You may use this clause if you do not disclose nonpublic personal information to any party, other than as permitted by the exceptions in §§ 313.14, and 313.15.

Sample Clause A–3

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A–4—Categories of Parties to Whom You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15, as well as when permitted by the exceptions in §§ 313.14, and 313.15.

Sample Clause A–4

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [*provide illustrative examples, such as ''mortgage bankers, securities broker-dealers, and insurance agents''*];
- Non-financial companies, such as [*provide illustrative examples, such as ''retailers, direct marketers, airlines, and publishers''*]; and
- Others, such as [*provide illustrative examples, such as ''non-profit organizations''*].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A–5—Service Provider/Joint Marketing Exception

You may use one of these clauses, as applicable, to meet the requirements of § 313.6(a)(5) related to the exception for service providers and joint marketers in § 313.13. If you disclose nonpublic personal information under this exception, you must describe the categories of nonpublic personal information you disclose and the categories of third parties with whom you have contracted.

Sample Clause A–5, Alternative 1

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–5, Alternative 2

We may disclose all of the information we collect, as described [*describe location in the notice, such as ''above'' or ''below''*] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A–6—Explanation of Opt Out Right (Institutions that Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(6) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–6

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [*describe a reasonable means of opting out, such as ''call the following toll-free number: (insert number)''*].

A–7—Confidentiality and Security (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(8) to describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A–7

We restrict access to nonpublic personal information about you to [*provide an appropriate description, such as ''those employees who need to know that information to provide products or services to you''*]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

By direction of the Commission.

Approved by the Commission on May 12, 2000.

Donald S. Clark,

Secretary.

[FR Doc. 00–12755 Filed 5–23–00; 8:45 am]

BILLING CODE 6750–01–P