SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 248

[Release Nos. 34–42974, IC–24543, IA–1883; File No. S7–6–00]

RIN 3235–AH90

Privacy of Consumer Financial Information (Regulation S–P)

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission is adopting Regulation S–P, privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act. Section 504 requires the Commission and other federal agencies to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. Under the Gramm-Leach-Bliley Act, a financial institution must provide its customers with a notice of its privacy policies and practices, and must not disclose nonpublic personal information about a consumer to nonaffiliated third parties unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure. The Act also requires the Commission to establish for financial institutions appropriate standards to protect customer information. The final rules implement these requirements of the Gramm-Leach-Bliley Act with respect to investment advisers registered with the Commission, brokers, dealers, and investment companies, which are the financial institutions subject to the Commission's jurisdiction under that Act.

DATES: *Effective Date:* This regulation is effective November 13, 2000.

Compliance Dates: Compliance will be mandatory as of July 1, 2001. Joint marketing and service agreements in effect as of July 1, 2000 must be brought into compliance with § section 248.13 of Regulation S–P by July 1, 2002.

FOR FURTHER INFORMATION CONTACT: For information regarding the rules as they relate to brokers or dealers, contact George Lavdas or Jerome Roche, Office of Chief Counsel, Division of Market Regulation, (202) 942–0073, or regarding the rules as they relate to investment companies or registered investment advisers, Penelope W. Saltzman or Hugh P. Lutz, Office of Regulatory Policy, (202) 942–0690, Division of Investment Management, Securities and Exchange Commission, 450 5th Street, NW., Washington, DC 20549.

SUPPLEMENTARY INFORMATION: The Securities and Exchange Commission (the ''Commission'') today is adopting new Regulation S–P, 17 CFR 248.1–248.30, under Title V of the Gramm-Leach-Bliley Act [Pub. L. No. 106–102, 113 Stat. 1338 (1999), to be codified at 15 U.S.C. 6801–6831], the Securities Exchange Act of 1934 [15 U.S.C. 78] (''Exchange Act''), the Investment Company Act of 1940 [15 U.S.C. 80a] (''Investment Company Act''), and the Investment Advisers Act of 1940 [15 U.S.C. 80b] (''Investment Advisers Act'').

Table of Contents

I. Background

Subtitle A of Title V of the Gramm-Leach-Bliley Act (''G–L–B Act'' or the ''Act''), captioned Disclosure of Nonpublic Personal Information (''Title V''), limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. Title V also requires the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision (collectively, the ''Banking Agencies''), Secretary of the Treasury, National Credit Union Administration, Federal Trade Commission (collectively with the Banking Agencies, the ''Agencies''), and the Commission, after consulting with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, to prescribe regulations necessary to carry out the purposes of Title V.[1]

Commission representatives participated with representatives from the Agencies in drafting rules to implement Title V. As required by the G–L–B Act, the rules we are adopting today are, to the extent possible, consistent with and comparable to the rules adopted by the Agencies.[2] Regulation S–P contains rules of general applicability that are substantially similar to the rules adopted by the Agencies. The rules also contain examples that illustrate the application of the general rules. These examples differ from those used by the Agencies in order to provide more meaningful guidance to the financial institutions subject to the Commission's jurisdiction.

Title V also requires the Commission (and each of the Agencies) to establish appropriate standards for financial institutions subject to their jurisdiction to safeguard customer information and records. Regulation S–P includes requirements for investment advisers registered with the Commission (''registered advisers''), brokers, dealers (collectively, ''broker-dealers''), and investment companies (''funds'') to adopt appropriate policies and procedures that address safeguards to protect this information.[3]

II. Overview of Comments Received

On March 2, 2000, the Commission issued a notice of proposed rulemaking (the ''proposal'' or ''proposed rules'').[4] The Commission received a total of 115 comments in response to the proposal.[5] Of these, approximately 14 were from individuals, virtually all of whom encouraged the Commission to provide greater protection of individuals' financial privacy. Many individuals noted their concerns generally about the

[1] G–L–B Act § 504(a)(1).

[2] *See* G–L–B Act § 504(a). The Banking Agencies published a joint release adopting rules to implement Title V earlier this month. Privacy of Consumer Financial Information, 65 FR 35162 (June 1, 2000) (''Banking Agencies' Release''). The National Credit Union Administration approved its final rules on May 8, 2000 [Privacy of Consumer Financial Information; Requirements for Insurance, 65 FR 31722 (May 18, 2000)]. The Federal Trade Commission adopted its privacy rules on May 12, 2000 [Privacy of Consumer Financial Information, 65 FR 33646 (May 24, 2000)].

[3] Under the G–L–B Act, investment advisers registered with the States are regulated by the Federal Trade Commission. *See* G–L–B Act § 505(a)(7).

[4] Privacy of Consumer Financial Information (Regulation S–P), Exchange Act Release No. 42484 (Mar. 2, 2000) [65 FR 12354 (Mar. 8, 2000)] (''Proposing Release'').

[5] The Banking Agencies, FTC, and NCUA received a total of 8,126, 640, and 99 comments, respectively, in response to their proposed rules.

loss of privacy and the receipt of unwanted solicitations by marketers.[6]

Other commenters advocated that we extend privacy protections in a number of ways. These suggestions included requiring (i) financial institutions to provide consumers with access to information about them maintained by the institutions and the opportunity to correct errors, (ii) more detailed disclosures of the information collected and disclosed, and (iii) disclosures of a financial institution's privacy policies and practices earlier in the process of establishing a customer relationship.

The National Association of Insurance Commissioners (''NAIC'') submitted a comment on behalf of the State insurance authorities that generally supported the Commission's proposed rules. The NAIC also proposed various measures to provide certain protections for consumers, such as specifying means to exercise the right to opt out of the disclosure of information. The NAIC further advised the Commission 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 (''HIPAA'') of 1996.[7]

We received approximately 20 letters from broker-dealers, funds, registered advisers, insured depository institutions, bank holding companies, and their representatives.[8] These commenters suggested many changes to the proposed rules. The most common suggestions included: (i) Extending the effective date of the rules; (ii) amending the definition of ''nonpublic personal information'' to focus more clearly on what they believe is ''financial'' information; (iii) streamlining information required in the initial and annual disclosures; (iv) clarifying how one or more of the statutory exceptions operate; (v) revising or clarifying the definitions of ''consumer'' and ''customer''; and (vi) adding flexibility to provide initial notices at some point other than ''prior to'' the time a customer relationship is established.

We have modified the proposed rules in light of the comments received.[9] These comments, and our responses to them, are discussed in the following section-by-section analysis.

III. Section-by-Section Analysis

The final Regulation presents the various sections in five subparts that consist of related sections. Related concepts are grouped together to make the rules easier to follow. A comparison table is included in section V to assist readers in locating provisions that appeared in the proposal. We also have added an Appendix to the final rules, setting out sample disclosures for broker-dealers, funds, and registered advisers to consider.

Section 248.1 Purpose and Scope

We are revising section 248.1, which identifies the purposes and scope of the rules. As stated in the proposal, the rule is intended to require a broker-dealer, fund, or registered adviser to provide notice to customers about its privacy policies and practices; to describe the conditions under which the institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and to provide a method for consumers to prevent the 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 rules.

Most of the comments received on this section focused on the scope of the rules. Several commenters suggested that the Commission clarify how the rules apply to insurance companies. Section 505 of the G–L–B Act sets out the Commission's enforcement authority with respect to broker-dealers, funds, and registered advisers. The section explicitly excludes ''persons providing insurance'' from the Commission's (and the Agencies') enforcement authority (and, by operation of section 504(a)(1) of the G–L–B Act, from the Commission's and the Agencies' rulemaking authority). We believe that the G–L–B Act relies on the States to enforce Title V with respect to any insurance activities conducted by broker-dealers, funds, or registered advisers. Consistent with this reading of the statute, the final rule excludes the provision of insurance by a broker-dealer, fund, or registered adviser from the scope of Regulation S–P. If the insurance product also is a security, however, any broker-dealer or fund that provides that security, or registered adviser that provides advice with respect to that security is subject to Regulation S–P.[10] In addition, insurance company separate accounts that are ''investment companies'' under the Investment Company Act are subject to this part.[11]

Several commenters stated that Regulation S–P should apply to foreign financial institutions that solicit business from individuals in the United States. As adopted, the requirements of Regulation S–P apply to any broker-dealer, fund, or investment adviser that is registered with the Commission, regardless of whether its consumers are U.S. persons or non-U.S. persons, and regardless of whether it conducts its activities through U.S. or non-U.S. offices or branches.[12] We also have decided not to apply Regulation S–P to any foreign (or ''non-resident'') broker-dealer or fund that is not registered with the Commission. Despite the broad reach of the U.S. federal securities laws,[13] we believe it would be impractical to apply Regulation S–P to those foreign unregistered entities. If a foreign broker-dealer or fund conducts activities through U.S. interstate commerce in a manner that subjects it to the registration requirements of the U.S. securities laws, it is subject to those requirements and any other applicable protections to investors, such as anti-fraud protections. We do not believe that subjecting these unregistered entities to the obligation to provide the privacy and opt out notices under Regulation S–P would add to the protections provided to investors under the G–L–B Act. As noted above,

[6] Commenters also requested that the Commission support legislation that the commenters believe would provide additional protections. In addition, the Commission received a comment letter from the Congressional Privacy Caucus, which encouraged the Commission to exercise its rulemaking authority to provide more protections than were proposed. The Chairman of the Commission also received two letters signed by several members of Congress, and a third letter from other commenters, which urged the Commission not to delay the compliance date of the final rules until July 1, 2001.

[7] *See* Standards for Individually Identifiable Health Information, 64 FR 59918 (Nov. 3, 1999) (as amended by 65 FR 427 (Jan. 5, 2000)).

[8] Representatives of a wide variety of other interests, including the health care industry, retail merchants, insurance companies, credit bureaus, and higher education, also submitted comment letters.

[9] We also have included a guide to assist broker-dealers, funds, and registered advisers in their efforts to comply with the privacy rules. *See infra* section VI.

[10] *See infra* discussion of sections 248.3(j), (k) (noting that variable annuities and variable life insurance contracts are insurance products and securities).

[11] *See infra* section 248.3(r).

[12] The Regulation also applies to any unregistered broker, dealer or fund in the United States. *See* section 248.1. In accordance with the G–L–B Act, however, Regulation S–P does not apply to any investment adviser that is not registered with the Commission. *See* G–L–B Act §§ 505(a)(5) (Commission has jurisdiction over broker-dealers, funds, and registered advisers); 505(a)(7) (Federal Trade Commission has jurisdiction over financial institutions not subject to the specific jurisdiction of the federal functional regulators). We also note that the privacy rules of Banking Agencies do not apply to foreign offices of financial institutions. *See, e.g.*, Banking Agencies' Release, sections 40.1, 216.1, 332.1, 573.1.

[13] *See, e.g.*, *Alfadda* v. *Fenn*, 935 F.2d 475 (2d Cir.), *cert. denied*, 502 U.S. 1005 (1991); *see also Steele* v. *Bulova Watch Co.*, 344 U.S. 280 (1952).

however, if a foreign broker-dealer, fund, or investment adviser decides to register with the Commission, it would be required to comply fully with Regulation S–P.[14]

Several commenters suggested that the rule should not apply to entities that must comply with regulations proposed by HHS to implement the HIPAA.[15] We do not believe that broker-dealers, funds, or registered advisers would be subject to any rules HHS has proposed under HIPAA regarding protected health information. We recognize, however, that there could be areas of overlap between the rules adopted by HHS under HIPAA and the privacy rules. After HHS publishes its final rules, we will consult with HHS to avoid the imposition of duplicative or inconsistent requirements.

Section 248.2 Rule of Construction

We are revising section 248.2, which sets out a rule of construction intended to clarify the effect of the examples used in the rules, to include the sample clauses in the Appendix to the rules. As noted in the Proposing Release, the examples (and the sample clauses) are not intended to be exhaustive; rather, they are intended to provide guidance about how the rules would apply in specific situations.[16]

Commenters generally agreed that examples are helpful in clarifying how the rules will work in specific circumstances. Some commenters also suggested that we include more examples, and provide examples of model disclosures. 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 rules in other ways. Other commenters also requested that we treat the examples as safe harbors or establish a presumption that compliance with the examples constitutes compliance with the rules. Others stated that the examples ought to be identical in each privacy regulation adopted by the Commission and the Agencies.

We agree that more examples would be helpful, and have included additional examples in appropriate places throughout the rules. We also have provided sample clauses in the Appendix to assist broker-dealers, funds, and registered advisers in drafting privacy notices. The sample clauses are provided to illustrate the level of detail we believe is appropriate. We caution financial institutions against relying on the sample disclosures without determining the relevance or appropriateness of the disclosure for their operations. We have 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.[17]

We have not added a statement in the final rule regarding a financial institution's ability to comply with the rules in ways other than as suggested in the examples. The rule states that the facts and circumstances of each individual situation will determine whether compliance with an example constitutes compliance with the applicable rule.[18] The examples and the sample clauses do not provide a safe harbor.[19] Nevertheless, we believe that, when read together, the rule of construction, examples, and sample clauses provide broker-dealers, funds, and registered advisers sufficient guidance on ways to comply with the rules as well as sufficient flexibility to comply with the regulation in ways appropriate for the institution.

Section 248.3 Definitions

(a) *Affiliate.* We are adopting the definition of ''affiliate'' as proposed. The rule incorporates the definition of ''affiliate'' in the G–L–B Act.[20] An affiliation exists when one company ''controls'' (as defined in section 248.3(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 proposed rule also provided that a broker-dealer, fund, or registered adviser would be considered an affiliate of another company if the other company is regulated under Title V by one of the Agencies, and under that Agency's rules, the other entity would be affiliated with the broker-dealer, fund, or registered adviser. Few commenters addressed this definition, and none disagreed with it.

(b) *Broker.* We are adopting the definition of ''broker'' as proposed. The definition incorporates the meaning of ''broker'' in the Exchange Act. One commenter suggested that the definition exclude foreign banks and savings institutions because they will be subject to the privacy rules of the Banking Agencies.[21] We disagree, and the rule does not include this exception.[22] Brokers registered with the Commission include foreign entities that may not be subject to the Banking Agencies' privacy rules, which do not extend to foreign entities that do not have offices within the United States.[23]

(c) *Clear and conspicuous.* We are revising the definition of ''clear and conspicuous'' in response to issues raised by commenters. The proposed rules required various notices to be ''clear and conspicuous,'' and defined the 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 Proposing Release, each financial institution would retain the flexibility to decide for itself how best to comply with this requirement.[24]

We received a large number of comments on the proposed definition. Several commenters favored adopting the definition as proposed, with some advocating that the final rule include a requirement that disclosures 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

[14] We note that a foreign broker-dealer, fund, or investment adviser that registers with the Commission also must comply with regulatory requirements concerning service of process in the United States. *See* Exchange Act rule 15b1–5(a) [17 CFR 240.15b1–5(a)] (requiring foreign broker-dealer that registers with the Commission to consent to service of process in the United States). *See also* Investment Company Act rule 7d–1(b)(7) [17 CFR 7d–1(b)(7)]; Investment Advisers Act rule 0–2 [17 CFR 275.0–2].

[15] *See supra* note 7.

[16] *See* Proposing Release, *supra* note 4, at discussion of section 248.2.

[17] The sample disclosures address solely the level of detail required and do not attempt to provide guidance on issues such as type size, margin width, or other characteristics that affect whether a notice is clear and conspicuous.

[18] *Cf.* Banking Agencies' Release, *supra* note 2, at sections 40.2, 216.2, 332.2, 573.2 (''Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this part.'').

[19] *Compare* Banking Agencies' Release, *supra* note 2, sections 40.2, 216.2, 332.2, 573.2.

[20] G–L–B Act § 509(6).

[21] *See supra* discussion of section 248.2. We are unaware of any savings institution that is registered as a broker and would be subject to Regulation S–P.

[22] *See also supra* discussion of section 248.1 (privacy rules apply to the foreign offices of registered broker-dealers, funds, and advisers, in addition to the U.S. offices of all broker-dealers, funds, and registered advisers).

[23] Banking Agencies' Release, *supra* note 2, sections 40.1(b), 216.1(b), 332.1(b), 573.1(b).

[24] *See* Proposing Release, *supra* note 4, at discussion of proposed section 248.3(c).

with requirements that disclosures mandated by other laws be clear and conspicuous. Several commenters stated that the definition is inconsistent with requirements in other consumer protection regulations such as Regulation Z[25] and the Truth in Savings regulation,[26] which require only that a disclosure be reasonably understandable.[27] A few commenters questioned how the requirement would work in a document that contains several disclosures that are required to be clear and conspicuous, while others raised questions about how a disclosure may be clear and conspicuous on an Internet web site.

New standard for ''clear and conspicuous.'' The proposed definition developed the concept of ''clear and conspicuous.'' The phrase ''designed to call attention to the nature and significance of the information contained'' was intended to provide meaning to the term ''conspicuous.'' We believe that this standard will result in notices to consumers that communicate effectively the information consumers need in order to make an informed choice about the privacy of their information, including whether to open a brokerage account, purchase fund shares, or enter into an advisory contract with an adviser.

Examples of ''clear and conspicuous.'' We recognize that many of the examples are imprecise. We believe, 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 broker-dealer, fund, or registered adviser may make a disclosure clear and conspicuous. We note that the examples do not mandate how to make a disclosure clear and conspicuous. 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 concerns about the imprecision of the examples, we have incorporated several of the commenters' suggestions in the final rule for ways to make the guidance more helpful.[28]

Combination of several notices. Commenters stated that a document may combine different types of disclosures that are subject to specific disclosure requirements under different regulations. For example, a fund that includes a privacy notice in its prospectus would have to make the privacy notice clear and conspicuous, and would have to prepare the prospectus according to certain standards under the Securities Act of 1933.[29] The final rule provides an example of how a financial institution may make privacy disclosures conspicuous, including privacy disclosures that are combined in a document with other information.[30] In order to avoid the potential conflicts between two different rules requiring different sets of disclosures that are subject to different standards, the final rule does not mandate precise specifications for presenting various disclosures.

Disclosures on Internet web pages. Several commenters requested guidance on how they may clearly and conspicuously disclose privacy-related information on their Internet sites. Disclosures over the Internet may present some issues that will not arise in paper-based disclosures. Consumers may view various web pages within a financial institution's web site in a different order each time they access the site, aided by hypertext links. Depending on the 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 example concerning Internet disclosures states that broker-dealers, funds, and registered advisers 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, hypertext links, or sound) do not distract attention from the notice.[31] The examples also note that the institution should place a notice or a conspicuous link on a screen that consumers frequently access, such as a page on which consumers conduct transactions.

There is a range of approaches a broker-dealer, fund, or registered adviser could use based on current technology. For example, a broker-dealer could use a dialog box that pops up to provide the disclosure before a consumer provides information to a financial 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.

(d) *Collect.* We are revising the definition of ''collect'' to clarify the scope of the term.[32] The G–L–B Act requires a financial institution to disclose in its initial and annual notices 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 broker-dealer, fund, or registered adviser must include in its notices and to clarify that the obligations arise regardless of whether the 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.'' We disagree that information should not be deemed to be collected simply because it is not retrievable in an automated fashion. We believe that the method of retrieval is irrelevant to whether information should be protected under the rule. We agree, however, that the scope of the regulation should be refined, and have changed the definition of ''collect'' by using language from the Privacy Act of 1974.[33]

Other commenters requested that the rule clarify that information that a broker-dealer, fund, or registered adviser receives but then immediately passes along without retaining a copy, is not ''collected.'' We believe that merely receiving information without retaining 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.

(f) *Company.* We received no substantive comments on the proposed definition of ''company'' and are adopting it as proposed.[34]

(g) *Consumer.* We are adopting as proposed the definition of ''consumer,''

[25] 12 CFR part 226.

[26] Regulation DD, 12 CFR part 230.

[27] 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.''

[28] *See* section 248.3(c)(2).

[29] *See* 17 CFR 230.421(b).

[30] *See* section 248.3(c)(2)(ii)(E). Because we believe that privacy disclosures may be clear and conspicuous when combined with other disclosures, the rule does not mandate that privacy disclosures be provided on a separate piece of paper. The requirement is not necessary and would significantly increase the burden on financial institutions.

[31] Section 248.3(c)(2)(iii).

[32] *See* section 248.3(d).

[33] 5 U.S.C. 552a.

[34] See section 248.3(f).

and are revising the examples under the definition in response to issues raised by commenters. The G–L–B Act distinguishes ''consumers'' from ''customers'' for purposes of the statute's notice requirements. A broker-dealer, fund, or registered adviser 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.[35] We received a large number of comments on this proposed definition that raised questions about how the definition would apply in a variety of situations.

Evaluation of a request for a financial product or service. The proposal 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.[36] Because ''financial product or service'' includes a financial institution's evaluation of an application or request to obtain a financial product or service, a person becomes a consumer even if the application or request is denied or withdrawn.[37] The examples for the definition of ''consumer'' clarify that a consumer includes an individual who provides nonpublic personal information when seeking to obtain brokerage or investment advisory services. For example, an investor who provides nonpublic personal information to several registered advisers (whether orally or in writing) in seeking financial advisory services would be a consumer of each registered adviser, even if the investor does not enter into an advisory contract with any of the advisers.

Many commenters disagreed that someone should be deemed a consumer of a financial institution by virtue of the institution evaluating nonpublic personal information provided by the individual in an application or otherwise. These commenters maintained that the individual has not obtained a financial product or service, as is required by the G–L–B Act. We believe, however, that a ''financial product or service'' includes the evaluation of information an individual provides to the financial institution in order to obtain some other financial product or service. Broker-dealers, funds, and registered advisers frequently provide a range of services in connection with the delivery of a financial product, including the evaluation of information provided by an individual. The evaluation may be the sole financial product or service delivered, or one of several services provided in connection with establishing a customer relationship. For example, an investor who seeks to invest in certain investment products, such as stock options, must provide a broker-dealer or registered adviser with nonpublic personal information in connection with the request. Based on this nonpublic personal information, the broker-dealer or registered adviser may open an account for the investor, but deny his or her request to invest in options. Whether the evaluation is the sole product or service or one of several, the institution's evaluation of the individual's information is a separate financial product or service.

The proposed definition of ''consumer'' also is consistent with one of the primary purposes of Title V: To enable an individual to restrict a financial institution from sharing nonpublic personal information about the individual with a nonaffiliated third party. The information an individual provides 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, we have retained in the examples in the definition of ''consumer'' an individual who provides nonpublic personal information to a broker-dealer or investment adviser in connection with obtaining brokerage or investment advisory services.[38]

Loan sales. Several commenters requested clarification of circumstances in which a borrower becomes a consumer. The final rule provides that a person will be a consumer of any entity that holds ownership or servicing rights to an individual's loan.[39] We believe that financial institutions that own or service a loan provide 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. The final 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 maintained that an individual should not be considered to be a consumer of an entity that is acting as agent for a financial institution.[40] These commenters noted that the financial institution that hires the agent is responsible for that agent's conduct in carrying out the agency responsibilities. We agree and continue to believe that the broker-dealer, fund, or registered adviser has a consumer relationship, even if the institution uses agents to help it deliver its products or services. For example, fund consumers would not become consumers of the fund's transfer agent that services the fund's customer accounts. The final rule retains the examples addressing clearing agents and provides a more general example to illustrate this principle.[41]

Legal representative. We also agree with the suggestion by several commenters that the definition of ''consumer'' should clarify that a financial institution may satisfy the obligations stemming from a consumer relationship by dealing either with the individual who obtains a financial product or service from a financial institution or that individual's legal representative. We do not intend that the rule require a financial institution to send opt out and initial notices to *both* the individual and his or her legal representatives, and have amended the final rule accordingly.[42]

Trusts. We 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 Commission generally to exempt a financial institution from the requirements of the rules when it acts as a fiduciary or, in the alternative, to clarify the categories of individuals who 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

[35] *See* G–L–B Act § 502(a). *See also* sections 248.14 and 248.15. By contrast, the broker-dealer, fund, or registered adviser 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. G–L–B Act § 503(a).

[36] *See* proposed section 248.3(g)(1).

[37] *See* discussion of section 248.3(o) below.

[38] *See* section 248.3(g)(2)(i).

[39] Those consumers may not be customers, however. *See infra* discussion of section 248.3 (explaining how the definition of ''customer'' will be applied in the loan context). *See* section 248.4(c)(2).

[40] *See* proposed section 248.3(g)(2)(iii).

[41] *See* section 248.3(g)(2)(iii), (v).

[42] Section 248.3(g)(1).

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 rules. In these commenters' view, the trust itself is the institution's ''customer,'' and therefore the rules 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. They 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 customer.

We believe that 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. We agree with the commenters who concluded that, when the financial institution serves as trustee of a trust, neither the grantor nor beneficiary is a consumer or customer under the rules. Instead, the trust itself is the entity that obtains the financial services, and the rules do not apply because the trust is not an individual.[43] We note that a financial institution that is a trustee assumes obligations as a fiduciary, including the duty to protect the confidentiality of the beneficiaries' information, that are consistent with the purposes of the G–L–B Act and enforceable under State law. Accordingly, we have excluded an individual who is a beneficiary of a trust or a plan participant in an employee benefit plan, from the definitions of ''consumer'' and ''customer.'' Nevertheless, we believe that an individual who selects a financial institution to be a custodian of securities or assets in an individual retirement account or individual retirement arrangement (''IRA'') is a ''consumer'' under the G–L–B Act. We have included examples in the rule that appropriately illustrate this interpretation of the G–L–B Act.[43]

Requirements arising from consumer relationship. While the proposed and final rules define ''consumer'' broadly, we note that this definition will not result in any additional burden to a broker-dealer, fund, or registered adviser if (i) no customer relationship is established and (ii) the institution does not intend to disclose nonpublic personal information about the consumer to nonaffiliated third parties. Under the approach taken in the final rule, a broker-dealer, fund, or registered adviser 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 sections 248.14 and 248.15. The institution may disclose a consumer's nonpublic personal information to nonaffiliated third parties under the final rule, if it delivers the requisite notices and the consumer does not opt out. Thus, the rule allows a financial institution to avoid all of the rule's requirements for consumers who are not customers if the institution chooses not to share information about the consumers with nonaffiliated third parties. Conversely, if a broker-dealer, fund, or registered adviser chooses to share consumers' nonpublic personal information with nonaffiliated third parties, the financial institution is free to do so, provided it notifies consumers about the sharing 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.

(h) *Consumer reporting agency.* We received no comments on the proposed definition of ''consumer reporting agency,'' and we are adopting it as proposed.[45] The definition incorporates the definition of ''consumer reporting agency'' in the Fair Credit Reporting Act.[46]

(i) *Control.* We are adopting the definition of ''control'' as proposed. ''Control'' means the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. In addition, ownership of more than 25 percent of a company's voting securities creates a presumption of control of the company. This definition is used to determine when companies are affiliated.[47] Under the definition, companies are considered to be affiliates regardless of whether the control is by a company or individual.

Some commenters suggested that the rule adopt the definition of control used in Form BD to determine when an entity is a ''control affiliate.''[48] Another commenter suggested a test that focuses solely on percent of stock owned in a company in order to avoid the uncertainties from a ''control-in-fact'' test. One commenter suggested alternative definitions based on (i) the ability to control the use of information in a company in which an ownership interest exists or (ii) a bright line 10 percent ownership test that also provided for aggregating the interests of credit unions and their wholly owned subsidiaries.

We believe that a test based only on stock ownership is unlikely to be flexible enough to address all situations in which companies should be considered to be affiliated. In addition, the proposed definition of control is consistent with the definition in Form BD, except that the definition in Form BD creates a presumption of control in

[43] Similarly, a trust, partnership, or personal corporation that has an account with a broker-dealer, fund, or registered adviser would not be a customer for purposes of the privacy rules because these entities are not individuals.

[44] *See* section 248.3(g)(2)(vii)–(viii), 248.3(k)(2)(i)(D). Three commenters also requested clarification in the examples on whether an individual who uses a financial tool that a financial institution makes available on the Internet is the institution's consumer. The commenters noted that individuals generally use these tools on a one-time or sporadic basis, and the tool typically does not require the user to enter his or her name or address. Thus, the information provided through the Internet tool is not personally identifiable. We agree that under these circumstances the individual would not be the institution's ''consumer'' and that these circumstances are covered in the examples under the definition of ''consumer'' and personally identifiable financial information. *See* section 248.3(g)(2)(ii), 248.3(u)(2)(ii)(B).

[45] *See* section 248.3(h). The definition is used in sections 248.6(c)(1)(iv), 248.12(a), and 248.15(a)(5) of the final rules.

[46] 15 U.S.C. 1681a(f).

[47] *See* discussion of section 248.3(a) above.

[48] *See* Form BD, Uniform Application for Broker-Dealer Registration, Explanation of Terms, ¶ 1. Form BD defines ''control'' to mean the power, directly or indirectly, to direct the management or policies of a company, whether through ownership of securities, by contract, or otherwise. In addition, there is a presumption of control for any person that (i) is a director, general partner, or officer exercising executive responsibility (or having similar status or functions); (ii) has the right to vote 25 percent or more of a class of voting securities or the power to sell or direct the sale of 25 percent or more of a class of voting securities; or (iii) in the case of a partnership, has the right to receive upon dissolution, or has contributed, 25 percent or more of the capital.

broader circumstances.[49] The rule limits the presumption of control to ownership of more than 25 percent of the voting securities, consistent with the definition of control in the Investment Company Act.[50] This definition does not prevent a finding of control-in-fact in the circumstances that create a presumption of control under the definition in Form BD.

(j), (k) *Customer, Customer relationship.* We received a large number of comments on the definition of ''customer'' and ''customer relationship.'' A ''customer'' is a consumer who has a ''customer relationship'' with a financial institution, and a ''customer relationship'' is a continuing relationship between a consumer and a broker-dealer, fund, or registered adviser under which 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 engaging in an isolated transaction that by itself would be insufficient to establish a customer relationship, such as when an individual opens a brokerage account solely for the purpose of liquidating or purchasing securities as an accommodation, *i.e.,* on a one-time basis, without the expectation of engaging in other transactions.

Point at which a consumer becomes a customer. Commenters criticized the vagueness of the standard for differentiating consumers from customers. 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.

We recognize that the distinction between consumers and customers will, in some instances, require a financial institution to make a judgment about whether a customer relationship is established. When an individual engages in a transaction and is not likely to expect further communication about that transaction from the financial institution (such as brokerage services as an accommodation to buy or liquidate securities), the individual will not have established a customer relationship as a result of that transaction. In other situations when a consumer typically would receive some measure of continued service following, or in connection with, a transaction (such as when a consumer opens a brokerage account, is the record owner of fund shares, or obtains investment advice), a customer relationship is established. We believe that the distinction set out in the proposed rule, as further clarified by the examples in the final rule of when a customer relationship is and is not established, provides a sufficiently clear line while retaining flexibility to address less clear-cut situations on a case-by-case basis.

Use of ''isolated transaction'' test. The final rule does not define the distinction between consumer and customer based solely on whether the transaction is an isolated event. We used this concept in an example in the proposed rule to illustrate one of the factors that may determine whether a relationship is of a continuing nature. Several commenters suggested that this approach was insufficiently precise to serve as a workable distinction between consumers and customers. We agree that the test may not be useful in all situations, but believe that it will help clarify the status of relationships in certain circumstances. Accordingly, the final rule retains the following example of an ''isolated transaction'': providing brokerage services as an accommodation to buy or liquidate securities without the expectation of engaging in further transactions does not establish a customer relationship.[51]

Purchase of insurance. Some commenters suggested that, in the context of financial institutions that engage in the sale of insurance and that are regulated by the Commission, the customer should be the policyholder and not the beneficiary. As discussed above, Regulation S–P does not apply to the provision of insurance by broker-dealers, funds, or registered advisers. A variable annuity or variable life insurance contract, however, is both an insurance product and a security.[52] We agree with the commenters, and the final rule includes an example of purchasing a variable annuity as one situation in which a customer relationship is formed.[53] In this case, the person obtaining a financial product or service from the financial institution is the person purchasing the annuity.[54]

Sales of loans. As noted above, several commenters raised questions about loan sales. They stated that when a financial institution sells the servicing rights for a loan to another financial institution, the borrower should not be considered a customer of both institutions. Commenters suggested that the entity with which the borrower communicates about the loan (*i.e.,* the servicer) could have the *customer* relationship with the borrower, and that the other institutions could have a *consumer* relationship with the borrower.

We believe that it is appropriate to consider that a loan transaction gives rise to only one customer relationship and 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, many of which might be from secondary market purchasers that the borrower did not know had any connection to his or her loan. We note, however, that a borrower will remain a consumer of the institution that transfers the servicing rights, as well as a consumer of any other institution that holds an interest in the loan.

Under the final rules, therefore, a financial institution will be considered to have established a customer relationship with any individual to whom it makes a loan.[55] If the institution transfers the servicing rights of that loan to another institution, the second institution will establish a customer relationship with the individual, and the first institution's customer relationship will end (if the relationship is based solely on the loan).[56] If the originating lender sells the loan but continues to service the loan, it will continue to have a customer relationship with the borrower, and the purchaser will have a consumer relationship with the borrower.[57] For example, a broker-dealer who purchases a loan, but not the servicing rights to the loan, will have a *consumer* relationship, but not a *customer* relationship, with the borrower.[58]

---

[49] *Id. See also* section 248.3(i).

[50] *See* 15 U.S.C. 80a–2(a)(9).

[51] *See* section 248.3(k)(2)(ii).

[52] *See e.g., SEC* v. *Variable Annuity Life Ins. Co.,* 359 U.S. 65 (1959) (variable annuities); Exemption of Certain Variable Life Insurance Contracts and Their Issuers from Federal Securities Laws, Investment Company Act Release No. 7644 (Jan. 31, 1973) [38 FR 4315 (Feb. 13, 1973)] (variable life contracts).

[53] *See* section 248.3(k)(2)(i)(E).

[54] These individuals could include a contract owner and could also include any other individual who has the rights of a contract owner, such as the ability to direct underlying investments.

[55] *See* section 248.3(k)(2)(i)(A) (consumer who has a brokerage account (including a margin account) has a continuing relationship with a broker-dealer).

[56] The originating lender will then have a *consumer* relationship with the borrower.

[57] In those circumstances, the borrower will be entitled to receive initial and annual notices from the loan servicer.

[58] A broker-dealer who purchases loans for securitization would have to provide notice and opt out to borrowers before sharing nonpublic personal information about the borrowers with nonaffiliated third parties, unless the sharing was necessary to effect or administer the securitization. *See* section 248.14(a)(3).

Fund shares purchased through an intermediary. Several commenters suggested that an individual who is the record owner of fund shares should not be a fund's ''customer'' if the fund is limited, under its contract with the intermediary who sold the shares, to servicing the investor's account. The commenters argue that these investors would be confused by receiving privacy notices from the fund. We proposed a ''bright line'' example of record ownership to establish the customer relationship because the fund clearly has nonpublic personal information about its record owners that is personally identifiable. We do not believe that an investor who receives account statements and other information from a fund that services the investor's account will be confused by receiving notices regarding the fund's privacy policies and practices. Moreover, an investor is unlikely to know whether a fund is contractually limited in its use of the investor's nonpublic personal information or whether those contract terms may change. For these reasons, we are adopting the proposed example that record owners of fund shares are the fund's customers.[59]

Fund complex. One commenter suggested that a customer of a fund should be considered a customer of the fund complex, which may include the fund's primary investment adviser, or that a fund customer, at least in some cases, should also be considered a customer of the fund's primary investment adviser. We noted in the Proposing Release that the record owner of fund shares has a customer relationship with both the fund and the principal underwriter (which is a broker-dealer) that sells the shares.[60] The customer relationship with the broker-dealer arises because the investor has an account with the broker-dealer, who provides financial services directly to the investor. By contrast, an investment adviser to a fund does not generally have an ongoing account relationship with each fund shareholder. Instead, it serves the fund shareholders indirectly through the portfolio management services it provides to the fund.

We recognize that the definition of ''customer'' may have disparate effects on the ability of some investment advisers to receive nonpublic personal information about fund investors. For example, if the underwriter of a fund is affiliated with the fund's investment adviser, the underwriter can share nonpublic personal information about its customers with the adviser. By contrast, if the underwriter is not affiliated with the fund's investment adviser, the underwriter can share this type of information only under an exception in section 248.13, 248.14, or 248.15, and the adviser's ability to reuse the information would be limited to the purpose for which it received the information. These limitations result from the language of the G–L–B Act, which defines affiliation in terms of ''control,'' and we are unwilling to modify the definition of ''customer relationship'' to alter the effect of that definition.[61] For these reasons, we believe that, in the absence of an advisory contract with the investor, a fund's primary investment adviser does not have a customer relationship with the fund's customers.[62]

Transferred accounts. One commenter requested clarification about whether an investor becomes a consumer of a broker-dealer when the consumer's account is transferred to the broker-dealer. An individual who has an account with a broker-dealer or a contract with a registered adviser has established a customer relationship with that broker-dealer or adviser. Thus, the investor is a customer of that broker-dealer or registered adviser, regardless of whether the account was transferred at the customer's request or as the result of a merger, acquisition, or assignment. Accordingly, the final rule includes an example that an individual is a customer of a broker-dealer or registered adviser if the individual's account is transferred to the broker-dealer or adviser.[63]

Trusts. The final rule adds an example to clarify that an individual will be deemed to establish a customer relationship when a broker-dealer, fund, or registered adviser acts as a custodian for securities or assets in an IRA.[64] This example is consistent with the explanation set out above in the discussion of ''consumer'' concerning trusts.[65]

(l) *Dealer.* We received no comments on the proposed definition of ''dealer'' and are adopting it as proposed. The definition incorporates the definition of dealer in the Exchange Act.[66]

(m) *Federal functional regulator.* We are defining the term ''federal functional regulator'' in place of ''government regulator.'' The proposal sought comment on a definition of ''government regulator'' which included each of the Agencies, the Commission, and State insurance authorities under the circumstances identified in the definition. This term was used in the exception in proposed section 248.15(a)(4) for disclosures to law enforcement agencies, ''including government regulators.''

For purposes of the privacy rules, this term is relevant in determining when an entity is an affiliate and when a broker-dealer, fund, or registered adviser may disclose information to a law enforcement agency.[67] The exception for disclosure as stated in the G–L–B Act uses the term ''Federal functional regulator,''[68] which is defined in the statute at section 509(2) and includes the Secretary of the Treasury for purposes of the exception permitting disclosures to law enforcement agencies. We have decided that it is appropriate to use the term ''federal functional regulator'' instead of ''government regulator.''

(n) *Financial institution.* We are adopting the definition of ''financial institution'' as proposed. The proposal 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 of 1956.[69] The G–L–B Act also defines ''financial institution,'' and the proposal excepted from the definition those entities the G–L–B Act also excepts.[70]

[59] One commenter also requested that the Commission except from the notice requirements closed-end funds whose information about record owners is limited to name, address, and number of shares held and who neither have affiliates nor share nonpublic personal information with third parties. The G–L–B Act does not exempt closed-end funds from privacy provisions of Title V. Although closed-end funds may bear the costs of mailing initial privacy notices to new customers, they can reduce the burden of annual notices by including them with a shareholder report. *See* discussion of section 248.3(c) (definition of ''clear and conspicuous'').

[60] *See* Proposing Release, *supra* note 4, at text following n.37.

[61] *See* G–L–B Act § 509(6).

[62] The investment adviser may receive nonpublic personal information about the fund's shareholders in connection with performing services on behalf of the fund or servicing the shareholders' accounts. The G–L–B Act permits a fund to share this information with the adviser if the adviser is an affiliate or if the adviser is a nonaffiliated third party. *See* G–L–B Act §§ 502(b)(2), (e). *See also* sections 248.13, 248.14.

[63] Section 248.3(k)(2)(i)(A).

[64] Section 248.3(k)(2)(i)(D).

[65] See supra discussion of section 248.3(g).

[66] 15 U.S.C. 78c(a)(5).

[67] The term also is used in the definition of ''affiliate.'' *See* section 248.3(a).

[68] *See* G–L–B Act § 502(e)(5).

[69] 69 12 U.S.C. 1843(k).

[70] G–L–B Act § 509(3); proposed section 248.3(m)(2). Two commenters requested that the rule clarify that an independent contractor registered representative of a broker-dealer is not a separate financial institution when acting in the capacity of a registered representative. We believe that the rules address this situation and need no further revision. An independent contractor

Continued

Commenters suggested that the final rule include additional exceptions from the definition, such as for securitization trusts, debt buyers, and credit bureaus. We have not included these exceptions in the final rule. We believe it is inappropriate to exclude many of the activities suggested by commenters because the objective of the suggested exclusions can be achieved in other ways. Even if an entity is a financial institution as that term is used in the G–L–B Act, it will not have any disclosure responsibilities under the Act or this rule if it does not provide a financial product or service to a consumer. In most of the situations posited by the commenters, the entity in question will not meet that test and therefore will fall outside the scope of the rules with respect to privacy disclosures.[71]

(o) *Financial product or service.* We are adopting the definition of ''financial product or service'' as proposed. The proposal defined the term as a product or service that a broker-dealer, fund, or registered adviser could offer by engaging in an activity that is financial in nature, or incidental to such a financial activity, under section 4(k) of the Bank Holding Company Act. An activity that is complementary to a financial activity, as described in section 4(k), was not included in the proposed definition of ''financial product or service.'' The proposal's definition included the broker-dealer, fund, or registered adviser's evaluation of nonpublic personal information collected in connection with a request by a consumer for a financial product or service even if the request ultimately is rejected or withdrawn.[72] It also included the distribution of information about a consumer for the purpose of assisting the consumer in obtaining a financial product or service.

Several commenters criticized the proposed definition and suggested that the evaluation of application information should not be considered a financial product or service. For the reasons discussed above regarding the definition of ''consumer,'' we continue to believe that it is appropriate to retain evaluation or brokerage of information as within the scope of financial products or services covered by the rules.

(q) *Investment adviser.* We received no comments on the proposed definition of ''investment adviser'' and are adopting it as proposed. The definition incorporates the definition of ''investment adviser'' under the Investment Advisers Act.[73]

(r) *Investment company.* We received no substantive comments on the proposed definition of ''investment company'' and are adopting it as proposed. The definition incorporates the definition of ''investment company'' under the Investment Company Act, whether or not the company is registered with the Commission.[74]

(s) *Nonaffiliated third party.* We are adopting the definition of nonaffiliated third party as proposed. The proposal defined the term as any ''person'' (including natural persons as well as corporate entities) except (i) an affiliate of a financial institution and (ii) 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 broker-dealer, fund, or registered adviser through that institution's merchant banking activities or insurance company activities would be a ''nonaffiliated third party'' of the broker-dealer, fund, or registered adviser.

We received very few comments in response to the proposed definition. One commenter requested that the final rule state 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. We disagree with this result. Instead, we believe 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, for example, if an employee of a bank is also an employee of a brokerage firm, information that employee receives in connection with a securities transaction conducted with the brokerage firm would be considered as received by the brokerage firm.

(t) *Nonpublic personal information.* We are revising the definition of ''nonpublic personal information.'' Section 509(4) of the G–L–B Act defines the term to mean ''personally identifiable financial information'' that is provided by a consumer to a financial institution, results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. The term 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 that is not publicly available information.'' The G–L–B Act excludes publicly available information (unless provided as part of the list, description, or other grouping described above), as well as any 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 rules implemented the definition of ''nonpublic personal information'' under the G–L–B Act by restating the categories of information described above. The proposed rules treated information as publicly available if a broker-dealer, fund, or registered adviser *could* obtain it from a public source. We also asked for comment on an approach that would have deemed information as ''publicly available'' only if a financial institution *actually* obtained it from a public source (''alternative approach'').[75] Most commenters supported the proposed approach to publicly available

registered representative is considered an ''associated person'' of a broker-dealer under the Exchange Act if the representative's activities are subject to control by the broker-dealer, such as when there is a principal and agent relationship. *See* Letter to Gordon S. Macklin, President, National Association of Securities Dealers, Inc. from Douglas Scarff, Director, Division of Market Regulation, Commission (June 18, 1982) (on file with the Commission). As discussed above, a broker-dealer's consumer is not considered a consumer of the broker-dealer's agent. *See* section 248.3(g)(2)(v). An independent contractor, however, also may be a registered adviser who as such, acts in a different capacity than as agent for the broker-dealer. In these circumstances, the registered representative is a different financial institution. Therefore, an investor who obtains investment advisory services from that registered representative acting as an investment adviser would be a consumer of the investment adviser.

[71] These entities will, however, be subject to the limits on reuse and redisclosure under section 248.11 with respect to any nonpublic personal information they receive from a nonaffiliated financial institution that has disclosure obligations under these rules.

[72] *But see* section 248.3(g)(2)(ii) (an individual is not a consumer of a broker-dealer, fund, or registered adviser if the individual provides the institution only with name, address, and general areas of interest in connection with a request for a prospectus, investment adviser brochure, or other information about financial products or services).

[73] 15 U.S.C. 80b–2(a)(11).

[74] 15 U.S.C. 80a–3. As noted in the Proposing Release, a business development company, which is an investment company but is not required to register with the Commission, is subject to Regulation S–P. *See* Proposing Release, *supra* note 4, at n.30. *See also* 15 U.S.C. 80a–2(a)(48). An entity that is not an ''investment company'' under the Investment Company Act, is not subject to Regulation S–P. *See* 15 U.S.C. 80a–3(c).

[75] The Banking Agencies (other than the Board of Governors of the Federal Reserve) and the Federal Trade Commission proposed alternative rule text for this approach. *See* Privacy of Consumer Financial Information, 65 FR 8770, 8790–91, 8804–05, 8811–12 (Feb. 22, 2000); Privacy of Consumer Financial Information, 65 FR 11174, 11189–90 (Mar. 1, 2000) (Federal Trade Commission proposal).

information. They noted that the proposed rule was consistent with the Act and would be far less burdensome on financial institutions. They also stated that any requirement that the information actually be obtained from a public source would impose a needless burden on financial institutions (by requiring, for instance, that a financial institution ''tag'' information it obtained from public records) and is not required by the Act. Other commenters advocated the alternative approach. They argued that the alternative approach would provide the greatest protection for consumers by treating any information the consumer gives to a financial institution to obtain a financial product or service as nonpublic personal information. 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 the alternative approach.

The final rule adopts an approach that we believe incorporates the benefits of both alternatives. As under the proposed rule, in the final rule information will be deemed to be ''publicly available'' and therefore excluded from the definition of ''nonpublic personal information'' if a broker-dealer, fund, or registered adviser reasonably believes that the information is lawfully made available to the general public from one of the three categories of sources listed in the rule.[76] The examples provided in the rule clarify when a broker-dealer, fund, or registered adviser has a reasonable belief that information is lawfully made available to the general public. For example, an institution would have a reasonable belief if (i) the institution has confirmed, or the consumer has represented, that the information is publicly available from a public source, or (ii) the institution has taken steps to submit the information, in accordance with its internal procedures and policies and with applicable law, to a keeper of federal, State, or local government records who is required by law to make the information publicly available.[77] The examples also state that a broker-dealer, fund, or registered adviser would have a reasonable belief that a telephone number is publicly available if the institution located the number in a telephone book or if the consumer told the institution that the number is not unlisted.[78] Moreover, the examples make clear that an institution may not assume information about a particular consumer is publicly available simply because that type of information is normally provided to a government record keeper and made available to the public by the record keeper, because the consumer may have the ability to keep that information non public or to screen his or her identity.

The approach of the final rule is based on the underlying principle that a consumer in many circumstances can control the public availability or identification of his or her information and that a financial institution therefore should not assume that the information about that customer is in fact publicly available. Thus, even though a lender typically enters a mortgage in public records in order to protect its security interest, when a borrower can maintain the privacy of his or her personal information by owning the property and obtaining the loan through a separate legal entity, the customer's name would not appear in the public record. In the case of a telephone number, a person may request that his or her number be unlisted. Thus, in evaluating whether it is reasonable to believe that information is publicly available, a financial institution must determine whether the consumer has kept the information or his or her identity from being a matter of public record.[79]

To implement the complex definition of ''nonpublic personal information'' that is provided in the statute, the final rule adopts a definition that consists, generally speaking, of (i) personally identifiable financial information, plus (ii) a consumer list or description or grouping of consumers (and publicly available information pertaining to the consumers) that is derived using any personally identifiable financial information that is *not* publicly available information. From that body of information, the final rule excludes publicly available information (except as noted above or if the information is disclosed in a manner that indicates that the individual is the institution's consumer) and any consumer list that is derived without using personally identifiable financial information that is not publicly available information.[80] Examples illustrate how this definition applies in the context of consumer lists.[81]

(u) *Personally identifiable financial information.* We are adopting the definition of ''personally identifiable financial information'' substantially as proposed. The proposed rule defined the term to include (i) information that a consumer provides a broker-dealer, fund, or registered adviser in order to obtain a financial product or service, (ii) information resulting from any transaction between the consumer and a broker-dealer, fund, or registered adviser involving a financial product or service, and (iii) information about a consumer that a broker-dealer, fund, or registered adviser 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 consumer of a broker-dealer, fund, or registered adviser as personally identifiable financial information. In essence, the proposed rules treated any personally identifiable information as ''financial'' if a broker-dealer, fund, or registered adviser obtained the information in connection with providing a financial product or service to a consumer. We noted in the Proposing Release that this interpretation may result in certain information being covered by the rules that may not commonly be considered intrinsically financial, such as health status.[82]

We received a large number of comments in response to the definition of ''personally identifiable financial information.'' Many commenters objected to including in the term certain identifying information that they did not view as ''financial,'' such as name, address, and telephone number. Many commenters argued that ''personally identifiable financial information'' should not include the fact that someone is a customer of a financial institution. These commenters noted that many customer relationships are matters of public record (such as would be the case, for instance, any time a transaction results in the recording 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. We continue to believe that it is appropriate to treat any information as ''financial'' information if a financial institution obtains it in order to provide

[76] *See* section 248.3(v)(1). *See also* 17 CFR 230.144A(d)(1), .903(b)(1)(i).

[77] Section 248.3(v)(2).

[78] *See* section 248.3(v)(3)(iii)(2).

[79] *Compare* Banking Agencies' Release, *supra* note 2, sections 40.3(p), 216.3(p), 332.3(p), 573.3(p) (definition of ''publicly available information'').

[80] *See* sections 248.3(t)(2).

[81] *See* section 248.3(t)(3).

[82] *See* Proposing Release, *supra* note 4, at discussion of proposed section 248.3(v).

a financial product or service. We also believe this approach is consistent with the G–L–B Act. Although the statute does not define the term ''financial,'' it does include a broad definition of ''financial institution'' used in the G–L–B Act, which encompasses a large number of entities (such as travel agencies, insurance companies, and data processors) that engage in activities not traditionally considered financial. 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 a financial institution uses in connection with providing a financial product or service is extremely broad and may include, for instance, medical information and other types of information that might not commonly be thought of as financial. It includes information a broker-dealer, fund, or registered adviser requests from the consumer, obtains from a transaction involving a financial product or service with the consumer, or otherwise obtains in connection with providing a financial product or service to a consumer. Thus, the information included in the definition of ''financial'' is information the broker-dealer, fund, or registered adviser has determined is relevant to providing a financial product or service.

We are sensitive to the concern expressed by several commenters about the need for ready access to identifying information to locate individuals who are attempting to evade their financial obligations. These commenters suggested that names, addresses, and telephone numbers should not be treated as financial information. We believe, however, that this information is financial, and is covered by the G–L–B Act. Broker-dealers, funds, and registered advisers rely on a broad range of information, including information such as addresses and telephone numbers, when providing financial products or services. Broker-dealers, funds, and registered advisers use location information to provide a wide variety of financial services, such as sending account statements and disbursing funds to a consumer. We concluded that it would be inappropriate to exclude certain items of information from the definition of personally identifiable financial information simply because a particular broker-dealer, fund, or registered adviser might not rely on those items when providing a particular financial product or service.[83]

Customer relationship as ''personally identifiable financial information.'' We disagree with those commenters who maintain that customer relationships should not be considered to be personally identifiable financial information. This information is ''personally identifiable'' because it identifies the individual as a customer of the institution. The information is financial because it reveals a financial relationship with the institution and the receipt of financial products or services from the institution.

Changes made to the definition. We have revised the definition of ''personally identifiable financial information'' 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 an information-collecting device from a web server, often referred to as a ''cookie.'' [84] This example illustrates one of the many ways that a financial institution may obtain information about a consumer in connection with providing a financial product or service to that consumer.

In addition, in response to many comments from the securities industry, the final rule also includes an example that clarifies that aggregate information (or ''blind data'') lacking personal identifiers is not covered by the definition of ''personally identifiable financial information.'' [85] We agree with the commenters who argued that this type of data does not ''identify'' any individual.

(v) *Publicly available information.* We are adopting the definition of ''publicly available information'' substantially as proposed. The proposal defined the term to include information that is lawfully available to the general 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 prospectuses and periodic shareholder reports). 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 previously explained in the discussion of ''nonpublic personal information,'' we have adopted the proposed approach in the final rule, but with additional clarifying provisions.

Many commenters questioned the appropriateness of excluding from the definition of ''publicly available information'' information that a person obtains over the Internet by using a password or complying with a similar restriction. These commenters noted that many Internet sites are available to a large number of people, each of whom needs a user name and identification number to access the sites. Several of these commenters suggested that it would be more appropriate to focus on whether the information was lawfully placed on the Internet.

We agree with these comments, and have revised 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, we have substituted a standard that requires the information, whether from the Internet or otherwise, to be available on an unrestricted basis. Information that an individual specifically requests be compiled, such as information that a locator or ''look up'' service provides with respect to a particular individual that may combine confidential information in addition to publicly available information, will not be considered available to the general public on an unrestricted basis, regardless of whether the information is provided over the Internet or otherwise. The rule also states that an Internet 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. One common use of passwords is to confine the access of web site users to specific, individual information. However, web site operators also may require user identifications and passwords as a method of tracking access rather than restricting access to the information available through the website. Internet service providers may charge fees to users to access the site rather than to restrict access to particular information. Other sites available to the general public, such as daily newspapers, also may charge a fee to access archived

[83] We note 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 information). An investment adviser's client list is an example of this type of information, even if the list includes clients' names, addresses, and telephone numbers that are otherwise publicly available. In circumstances in which a consumer does not opt out, a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party if the disclosure is consistent with the institution's opt out and privacy notices.

[84] *See* section 248.3(u)(2)(i)(F).

[85] *See* section 248.3(u)(2)(ii)(B).

information. Therefore, we believe 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.

We note that the concept of information being lawfully obtained was included in the proposal, and is retained in the final rule.[86] 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.

(w) *You.* We are adopting the definition of ''you'' largely as proposed. The proposed definition of ''you'' referred to broker-dealers, funds, and registered advisers, which are the entities within the Commission's jurisdiction under Title V. We are, however, revising the definition to clarify that the provision of insurance by financial institutions under the Commission's primary jurisdiction is not covered under these rules.[87]

A. Subpart A—Privacy and Opt Out Notices

Sections 248.4 through 248.9 of Regulation S–P include requirements concerning the delivery of initial and annual notices about the privacy policies and practices of a financial institution, and about the opportunity and methods for consumers to opt out of their institution's sharing of their nonpublic personal information with nonaffiliated third parties.

Section 248.4 Initial Privacy Notice to Consumers Required

We are revising the requirements relating to initial privacy notices to consumers, in response to issues raised by commenters. 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.[88] For consumers who are not customers, the notice must be provided before disclosing nonpublic personal information about the consumer to a nonaffiliated third party.[89]

The proposed rules 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. The rule required these disclosures to be clear and conspicuous and to accurately reflect the institution's privacy policies and practices. The proposal also set out rules governing when a customer relationship is established and how a financial institution is to provide notice.[90]

We received many comments raising concerns about proposed section 248.4. Most commenters from the securities industry raised questions about the time when initial notices must be provided, 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. Almost all the commenters from the securities industry 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 when a customer relationship is established. Some of 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.

Although we believe many commenters misinterpreted the proposed language concerning the timing for providing initial notices, we have revised the rule to clarify the requirement. The final rule states that, as a general rule, the initial notice must be given not later than the time when a financial institution establishes a customer relationship.[91] As stated in the Proposing Release, the initial notices may be provided at the same time a broker-dealer, fund, or registered adviser is required to give other notices, such as the requirement that credit terms in margin transactions be disclosed,[92] or that a registered adviser provide each client with a written disclosure statement (''brochure'') not later than the time of entering an investment advisory contract with the client.[93] This approach, like the approach taken in the proposed rule, strikes a balance between (i) ensuring that consumers will receive privacy notices at a meaningful point during the process of ''establishing a customer relationship'' and (ii) minimizing unnecessary burden on broker-dealers, funds, and registered advisers that may otherwise result if the final rule were to require financial institutions to provide consumers with a series of notices at various 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 offered several situations in which a customer relationship is established without direct contact between the consumer and the financial institution. The commenters stated that delivery of the initial notice *before* the customer relationship is established in these situations would be impractical. Commenters also indicated that in many circumstances requiring delivery at this time 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.

To accommodate the wide range of situations presented by the commenters, we have modified the examples of when subsequent delivery of the initial notice is appropriate, so that they now are more broadly applicable. As stated in the final rule in section 248.4(e), a broker-dealer, fund, or registered adviser may satisfy the delivery requirement by providing the initial notice within a reasonable time after establishing a customer relationship, in three instances. First, the institution may provide notice after the fact if the customer has not elected to establish the customer relationship.[94] This might occur, for example, when a brokerage account is transferred to another broker by a trustee selected by the Securities Investor Protection Corporation (''SIPC'') and appointed by a United States Court.[95] Second, a broker-dealer, fund, or registered adviser may send a notice after establishing a customer relationship when to do otherwise

[86] *See* section 248.3(v)(1).

[87] As noted above, however, broker-dealers and funds that provide insurance products that also are securities and registered advisers who provide advice with respect to those products will be subject to this part with respect to their provision of those securities and advice about those securities. *See supra* discussion of section 248.1.

[88] G–L–B Act § 503(a).

[89] G–L–B Act § 502(a).

[90] *See* proposed section 248.4.

[91] Section 248.4(a)(1).

[92] 17 CFR 240.10b–16. *See* Proposing Release, *supra* note 4, at text accompanying n.35.

[93] 17 CFR 275.204–3(b) (requiring delivery of the brochure (i) not less than 48 hours before entering into an investment advisory contract with the client or (ii) at the time of entering into the contract as long as the client has at least 5 business days to cancel the contract without penalty).

[94] *See* section 248.4(e)(1)(i).

[95] *See* 15 U.S.C. 78eee–78fff–1.

would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.[96] An example of this is when an investor requests over the telephone that a broker-dealer execute a securities trade. The final example states that delayed delivery is permissible when a nonaffiliated broker-dealer or registered adviser purchases fund shares or establishes a brokerage account on behalf of a customer.[97]

We note that in most situations, a broker-dealer, fund, or registered adviser should give the initial notice at a point when the consumer still has a meaningful choice about whether to enter into the customer relationship.[98] The exceptions listed in the examples, while not exhaustive, are intended to 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 broker-dealer, fund, or registered adviser should deliver the notice within a reasonable time thereafter. Several commenters requested that the final rule specify how many days a financial institution has in which to deliver the notice under these circumstances. However, we believe that a rule prescribing the maximum number of days would be inappropriate because (i) the circumstances of when an after-the-fact notice is appropriate are likely to vary significantly, and (ii) a rule that attempts to accommodate every circumstance is likely to provide more time than is appropriate in many instances. Therefore, we have retained the more general rule as set out in the proposal.[99]

As we noted in the Proposing Release, 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 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.[100]

New notices not required for each new financial product or service. Several commenters asked whether a new initial notice is required every time a consumer obtains a financial product or service from that broker-dealer, fund, or registered adviser. These commenters suggested that a consumer 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.

We agree that it would be burdensome, with little corresponding benefit to the consumer, 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 that a broker-dealer, fund, or registered adviser 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.[101]

Joint accountholders. We agreed with several commenters who recommended that the final rule state that a financial institution is not obligated to provide more than one notice to joint accountholders.[102] Accordingly, the final rule clarifies that one notice may be sent in connection with a joint account.[103] A broker-dealer, fund, or registered adviser may, in its discretion, provide notices to each party to the account. This situation might arise, for example, when a financial institution does not want one opt out election to apply automatically to all joint accountholders.[104]

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.[105]

As was stated in the Proposing Release, a financial institution may not fail to maintain the protections that it represents in the notice that it will provide.[106] We expect that broker-dealers, funds, and registered advisers will take appropriate measures to adhere to their stated policies and practices.

Section 248.5 Annual Privacy Notice to Customers Required

We are adopting largely as proposed the requirements relating to annual privacy notices to consumers. 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 rules 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.[107] The proposed rule noted that the rule 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.[108]

Many commenters from the securities industry requested that the final rule permit annual notices to be given each calendar year, instead of every 12 months. A few commenters recommended that the rule require notices 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, stating that a broker-dealer, fund, or registered adviser may select a calendar year as the

[96] *See* section 248.4(e)(1)(ii).

[97] *See* section 248.4(e)(1)(iii).

[98] *See, e.g,* section 248.9(b)(1)(iii) (example of reasonable expectation that consumer will receive actual notice of initial privacy notice on Internet web site provides that consumer acknowledges receipt of notice as a necessary step to obtaining a particular financial product or service).

[99] *See* section 248.4(e)(1).

[100] *See* Proposing Release, supra note 4, at discussion of proposed section 248.4.

[101] *See* section 248.4(d).

[102] A few 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, *see* 12 CFR part 202, and the Truth in Lending Act, 15 U.S.C. 1601. Commenters noted that under both Regulation B and Regulation Z, a financial institution is permitted to give one notice. The authorities cited include requirements that the financial institution give disclosures as appropriate to the ''primary applicant'' if readily apparent, *see* 12 CFR 202.9(f), or to a person ''primarily liable on the account.'' *See* 12 CFR 226.5(b).

[103] *See* section 248.9(g).

[104] *See* discussion of section 248.9 below on how to provide opt out notices.

[105] If the surviving or acquiring institution does not deliver new notices, it must honor any opt outs the predecessor or acquired institution received from consumers.

[106] Proposing Release, *supra* note 4, at section discussing proposed section 248.4.

[107] *See* section 248.5(a).

[108] Proposed section 248.5(c)(1).

12-month period within which notices will be provided, and deliver the first annual notice at any point in the calendar year following the year in which the customer relationship was established.[109] The final rule also requires that a broker-dealer, fund, or registered adviser apply the 12-consecutive-month period to its customers consistently.

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. These commenters argued 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.

We have not amended the final rule to permit this approach, for two reasons. First, we believe that the G–L–B Act requires a full set of disclosures to each customer once a year.[110] Second, the revisions to the disclosure provisions reflected in the final rule clarify that a broker-dealer, fund, or registered adviser is not required to provide a lengthy and detailed privacy notice. 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 broker-dealer, fund, or registered adviser to provide annual notices to customers over the institution's web site if the customer conducts transactions electronically and agrees to the electronic disclosures.[111] As a result, the final rule achieves much of the burden reduction sought by those requesting a short-form annual notice option.[112]

Section 248.6 Information To Be Included in Initial and Annual Privacy Notices

We are revising the requirements for information to be included in initial and annual privacy notices. The revisions clarify the level of detail required in these notices, and permit a ''short-form'' initial notice in certain circumstances.

Section 503 of the G–L–B Act identifies the items of information that a broker-dealer, fund, or registered adviser must include in its 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 broker-dealer, fund, or registered adviser may collect;
- The categories of nonpublic personal information that a broker-dealer, fund, or registered adviser may disclose;
- The categories of affiliates and nonaffiliated third parties to whom a broker-dealer, fund, or registered adviser discloses nonpublic personal information, other than those to whom information is disclosed under an exception in section 502(e) of the G–L–B Act;
- The broker-dealer, fund, or registered adviser's policies with respect to sharing information about former customers;
- The categories of information that are disclosed under 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 Fair Credit Reporting Act; and
- The institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.

We received a large number of comments concerning these requirements, and most made the points summarized below.

Level of detail required. Many commenters observed that the level of detail required by the proposed rule would result in lengthy, complicated, and confusing disclosures. These comments have led us to revise the rule to clarify the level of detail required in a financial institution's initial and annual disclosures.

We do not intend to require a broker-dealer, fund, or registered adviser to publish lengthy disclosures that precisely identify every type of information collected or shared, the name of every entity with which the institution shares information, and a complete description of the technical specifications of how the institution protects its customers' records or the identity of each employee who has access to those records. Instead, the rule is intended to require notices that provide consumers with the types of third parties with which a financial institution shares nonpublic personal information, the types of information it shares, and the other information about the institution's privacy policies and practices listed above. The final rule, like the proposal, permits a broker-dealer, fund, or registered adviser to comply with these notice requirements by describing its privacy policies and practices.[113] We believe that in most cases the initial and annual disclosure requirements can be satisfied by disclosures contained in a tri-fold brochure.

In response to commenters' concerns that consumers will not read long, detailed disclosures, we have revised the examples of the disclosures to clarify the level of detail that we think is appropriate. We have provided sample clauses in the Appendix to the rules, and have set out a compliance guide below in this release. Because the examples are not exclusive, the final rule permits a financial institution to use different categories than those provided in the examples, thereby providing additional flexibility for financial institutions in complying with the disclosure requirements. In addition, we have revised the language that precedes the items of information to be addressed in the initial notice, to clarify that a broker-dealer, fund, or registered adviser is required only to address those items that apply to the institution. Thus, for instance, if an investment adviser does not disclose nonpublic personal information to third parties, it may simply omit any reference to the categories of affiliates

[109] *See* section 248.5(a)(2).

[110] 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 Act. G–L–B Act § 503.

[111] *See also* discussion of section 248.9 below.

[112] Members of the banking industry also commented on the paragraph in this section regarding termination of a customer relationship and examples set forth in the Banking Agencies' proposing release. *See* section 248.5(b). We have made a technical revision to one of the examples in response to the only comment that specifically addressed the Commission's proposed examples. *See* section 248.5(b)(2)(iii).

[113] *See* section 248.6(e).

and nonaffiliated third parties to whom the institution discloses nonpublic personal information.

As noted in the Proposing Release, the required content is the same for both the initial and annual notices of privacy policies and practices.[114] 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.

Short-form initial notice. We have 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, we believe that the objectives of the statute can be accomplished in a less burdensome way than was proposed. Accordingly, we have exercised our exemptive authority under section 504(b) to create an exception to the general rule that a financial institution must provide both the initial and opt out notices to a consumer before disclosing nonpublic personal information about that consumer to nonaffiliated third parties.

Section 248.6(d) provides 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 must clearly and conspicuously state that the disclosure containing information about the institution's privacy policies and practices is available on request, and must provide one or more reasonable means by which the consumer may obtain a copy of the notice. We believe that the short-form is appropriate because a consumer who does not become a customer of a broker-dealer, fund, or registered adviser may have less interest in certain elements of the institution's privacy policies. Thus, the consumer may receive greater benefit from obtaining a short-form notice with the opt out notice, which informs the consumer about the categories of his or her information the institution may share and the categories of nonaffiliated third parties that may receive the information. The rule also requires a broker-dealer, fund, or registered adviser to provide a consumer who is interested in the more complete privacy disclosures with a reasonable means to obtain them.

Information about affiliate sharing. Several commenters suggested that the rule should not require that initial and annual notices include categories of affiliates with whom a financial institution shares information. These commenters noted that the Act 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 under the Fair Credit Reporting Act (''FCRA'').[115] These commenters concluded that the Commission and the Agencies, by expanding the disclosure requirements in the manner prescribed in the proposed rule, would be exceeding their rulemaking authority and imposing an unnecessary burden on financial institutions.

We believe that 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 in the section 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) states 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 the disclosures to provide more information about affiliate sharing than what may be required under the FCRA.[116] That history underscores the Congressional intent of ensuring that individuals are given the opportunity to make informed decisions about the privacy policies and practices of financial institutions. We believe that limiting the disclosures about affiliate sharing just to those disclosures that may be required under the FCRA would frustrate that purpose.[117]

[114] Proposing Release, *supra* note 4, at discussion of proposed section 248.6.

[115] *See* 15 U.S.C. 1681a(d)(2)(A)(iii). Section 603(d)(2)(A)(iii) of the FCRA 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, for instance, information from consumer reports and applications for financial products or services. In general, this information includes personal information provided directly by the consumer to the institution, such as income and assets, in addition to information contained within consumer reports.

[116] *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.'').

[117] Commenters from other industries who addressed the issue argued that a financial institution should not be required to include FCRA disclosures in its annual notices. To the extent that broker-dealers share information about margin loans, they may be subject to the FCRA. 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 rules implemented section 503(b)(4) of the G–L–B Act by requiring that a broker-dealer, fund, or registered adviser's initial and annual notice include any disclosures a financial institution makes under section 603(d)(2)(A)(iii) of the FCRA. Proposed section 248.6(a)(7). Several commenters noted that the FCRA requires disclosures of a consumer's right to opt out of affiliate sharing only once, and 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. These commenters maintain that the ''if any'' language of section 503(b)(4), read in the context of section 506, suggests that, because at most only one notice must be provided under the FCRA, section 503 should require only one FCRA disclosure under the privacy rules.

As discussed above, we believe that in order to comply with the requirement 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 share information with affiliates. 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. Failing to include this information and an explanation of how the opt out right may be exercised would make the disclosures incomplete.

In addition, 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, section 503 suggests that any disclosures that are required under the FCRA must be included in both the initial and annual notices.

We interpret the ''if any'' language as an acknowledgment that not all institutions provide FCRA notices because not all institutions engage in the type of affiliate sharing covered by the FCRA. We do not believe that requiring the FCRA notice to appear as part of the annual notice under the privacy rules, modifies, limits, or supersedes the

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. We received many comments expressing support for a number of the provisions in proposed section 248.6. For example, several commenters agreed 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 under one of the exceptions. Others agreed with the proposed flexibility to allow a disclosure to be based on current and contemplated information sharing. In light of these comments, we have adopted proposed section 248.6 with changes as discussed above. The final rule makes several other stylistic changes to the material in section 248.6 that are intended to make the rule easier to read.

Section 248.7 Form of Opt Out Notice to Consumers; Opt Out Methods

We are adopting as proposed the requirement that any opt out notice provided by a broker-dealer, fund, or registered adviser be clear and conspicuous and accurately explain the right to opt out.[118] The final rule also requires, as proposed, that a financial institution provide the consumer with a reasonable means by which to opt out, and honor an opt out election as soon as reasonably practicable. The rule also states that an opt out election survives until revoked by the consumer. In addition, we have adopted provisions to address 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. The final rule also includes stylistic changes to make it easier to read.

Joint accounts. We agree with the commenters who stated that a financial institution should have the option of providing one notice per account, regardless of the number of persons on the account, and the final rule includes a new section to address this issue.[119] Under the final rule, a financial institution may provide one initial, annual, and opt out notice per account. However, each of the accountholders must have the right to opt out. The final rule also requires a broker-dealer, fund, and registered adviser 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 accountholders or whether each accountholder is permitted to opt out separately.

Means of opting out. At the suggestion of many commenters, the final rule includes a provision that permits a broker-dealer, fund, or registered adviser to require that a consumer opt out through a specific means, if the means is reasonable for the consumer.[120] We recognize that a financial institution may not have systems in place or trained personnel to handle opt out elections at each point of contact between a consumer and financial institution and therefore may choose not to honor opt out elections communicated to the institution through means other than those specified for the consumer.

As was proposed, the examples provide that a broker-dealer, fund, or registered adviser may not require a consumer to write his or her own letter in order to opt out.[121] The final rule adds an example of a toll-free telephone number as another way by which financial institutions may allow consumers to opt out.[122]

Duration of opt out. Several commenters requested changes to the proposed provision concerning duration of an opt out.[123] They noted that a financial institution would be required to keep track of opt out elections if, for example, a person 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.

We agree with the commenters' suggestions. Under the final rule, a broker-dealer, fund, or registered adviser is 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 institution collected during, or related to, that relationship. That opt out will continue until the customer revokes it.[124] However, if the customer relationship terminates and a new one is established at a later point, the 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.[125]

Level of detail required in opt out notice. We are adopting as proposed the rule requirements for the form of the opt out notice.[126] A few commenters interpreted the proposal as requiring a more detailed disclosure of categories of nonpublic personal information and nonaffiliated third parties in the opt out notice than is required in the initial and annual notices.[127] We did not intend this result, and specifically referred to section 248.6 in the proposed opt out provision to address precisely this concern. 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 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 those disclosures in the opt out notice. In these circumstances, the rule requires only that when the opt out

operation of the FCRA; financial institutions will have exactly the same FCRA obligations following the effective date of the privacy rules as they had before. The only difference will be that, as 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 institution complies with the affiliate sharing provisions of the FCRA.

[118] *See* section 248.8(a).

[119] *See* section 248.7(d).

[120] *See* section 248.7(a)(2)(iv).

[121] *See* section 248.7(a)(2)(iii)(A).

[122] *See* section 248.7(a)(2)(ii)(D).

[123] *See* proposed section 248.8(e).

[124] *See* section 248.7(g)(1).

[125] *See* section 248.7(g)(2).

[126] *See* section 248.7(a)(1).

[127] *See* proposed section 248.8(a)(2)(i) (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 [section 248.6]'').

and privacy notices are read together, they clearly disclose the categories of nonpublic personal information the institution intends to share and the categories of nonaffiliated third parties with whom it will share.

One commenter suggested that, while a broker-dealer, fund, or registered adviser should have the option of providing an opt out notice that is sufficiently broad to cover anticipated disclosures, the 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. If the consumer does not opt out a second time, the institution would be free to disclose nonpublic personal information obtained in connection with that financial product or service.

We agree that a broker-dealer, fund, or registered adviser should have the flexibility to provide opt out notices that are either narrowly tailored to specific types of nonpublic personal information and types of nonaffiliated third parties or that are more broadly worded to anticipate future disclosure plans. We note, however, that when a consumer has elected to opt out of sharing certain nonpublic personal information, the opt out remains in effect until the consumer affirmatively revokes the opt out. Similarly, when a consumer opts out after receiving an opt out notice that is broad enough to cover the new type of information the institution intends to share, the consumer does not have to opt out again.

Time by which opt out must be honored. We are adopting in the final rule the proposed requirement that a financial institution comply with an opt out election ''as soon as reasonably practicable.'' [128] Many commenters asked us to clarify in the final rule when a financial institution must stop disclosing nonpublic personal information to nonaffiliated third parties after it receives an opt out. Suggestions for a more precise standard ranged from immediate to several months after receiving the opt out. We believe that a more general rule is appropriate in light of the wide range of practices among financial institutions. A broker-dealer, fund, or registered adviser might view a specific standard as a safe harbor in all circumstances and thus fail to implement an opt out as early as it could. In addition, a standard that reflects existing industry practices and capabilities is likely to become outmoded quickly as advances in technology increase efficiency. We therefore decline to adopt a more rigid standard.

Section 248.8 Revised Privacy Notices

We are adopting as proposed the rule regarding revised privacy notices.[129] The rule prohibits 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 rule also requires that these notices be accurate when given.[130] Thus, if a broker-dealer, fund, or registered adviser wants to disclose nonpublic personal information in a way that is not accurately described in its notices, the institution must provide new notices before disclosing that information. The rule also provides examples of when a new notice is required.[131]

Section 248.9 Delivering Privacy and Opt Out Notices

The requirements for delivery of initial, annual, and opt out notices were set out in three different sections of the proposed rules.[132] The final rules combine in one section the requirements for delivery of each type of notice.[133] The general provision requires that an institution provide a notice to a consumer in a manner such that the consumer can reasonably be expected to receive actual notice in writing, or, if the consumer agrees, electronically.[134]

Posting initial notices on an Internet web site. The final rule retains the proposed example of posting a notice on an Internet 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, as one way to comply with the rule.[135] A few commenters suggested that a financial institution be allowed to deliver initial notices simply by posting the institution's notice on its Internet web site. We believe that posting the notice on a web site alone would not be sufficient in all cases for a broker-dealer, fund, or registered adviser reasonably to expect that its consumers will receive the notice.[136] Accordingly, we have not expanded the rule beyond the circumstances described in the proposed example.

Posting annual notices on an Internet web site. At the suggestion of several commenters, the final rule clarifies that a broker-dealer, fund, or registered adviser may reasonably expect a customer who uses the institution's Internet web site to obtain financial products or services will receive actual notice if the customer has agreed to accept notices at the institution's web site, and if the institution continuously posts a current notice of its privacy policies and practices in a clear and conspicuous manner on the web site.[137] We agree 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. We also believe that this revision will reduce the burden on broker-dealers, funds, and registered advisers while ensuring that customers who transact business electronically will have continuous access to institutions' privacy policies and practices.

Householding. Two commenters requested that the Commission permit broker-dealers and funds to deliver a single privacy notice to consumers who share the same address (''householding''). The Commission currently permits householding of prospectuses and fund shareholder reports, and the commenters argue that the same justifications that support the existing householding rules, such as reducing the number of duplicate documents investors receive, would apply with respect to privacy notices.[138] We agree that householding is appropriate in certain circumstances, and the final rule adds an example that allows a broker-dealer or fund to consider that customers have actually received an annual privacy notice if the institution includes the notice with or in a prospectus or shareholder report delivered under conditions set forth in rules permitting householding of those documents.[139]

---

[128] *See* section 248.7(e).

[129] *See* section 248.8. The final rule is in a separate section for emphasis.

[130] *See* section 248.8(a)(1).

[131] *See* section 248.8(b).

[132] *See* proposed sections 248.4(d) (initial notice), 248.5(b) (annual notice), and 248.8(b) (opt out notice).

[133] *See* section 248.9.

[134] Section 248.9(a).

[135] *See* section 248.9(b)(1)(iii).

[136] Nevertheless, there may be circumstances in which an Internet web site notice might be delivered in a way that will enable the broker-dealer, fund, or registered adviser to reasonably expect that the consumer will receive it.

[137] *See* section 248.9(c)(i).

[138] *See* Delivery of Disclosure Documents to Households, Investment Company Act Release No. 24123 (Nov. 4, 1999) [64 FR 62540 (Nov. 16, 1999)]. The Commission also has proposed rule amendments to permit householding of proxy or information statements. *See* Delivery of Proxy and Information Statements to Households, Investment Company Act Release No. 24124 (Nov. 4, 1999) [64 FR 62548 (Nov. 16, 1999)]. The comment period on this proposal ended January 18, 2000.

[139] *See* section 248.9(c)(2).

The example requires that the annual privacy notice be delivered with or in a prospectus or shareholder report that is householded because we believe that customers whose disclosure documents are householded also would consent to having their annual privacy notices householded. We cannot assume that the same would be true for other customers. The example also limits householding to annual privacy notices because we believe that any reduction in the number of initial notices consumers might receive due to householding would be minimal. Individuals who share the same address may not become consumers of a broker-dealer, fund, or registered adviser at the same time.

Disclosures to customers requesting no communication. We received comment that the final rule clarify that a financial institution may honor a customer's request not to receive information from the institution about his or her relationship with the institution. The final rule clarifies that a broker-dealer, fund, or registered adviser need not send an *annual* privacy notice to a customer who affirmatively requests no communication from the institution, provided that the notice is available upon request.[140]

Reaccessing a notice. The final rule provides an example that permits a broker-dealer, fund, or registered adviser to provide only the current privacy notice on a web site to someone seeking to obtain the privacy notice after having received the initial notice.[141] This example responds to a request for clarification in the rule concerning potential confusion and burden that might result if the rule required a financial institution to make available every version of its privacy policies.

Joint notices. The final rule affirms that two or more financial institutions may provide a joint notice as long as the notice is accurate with respect to each institution.[142] This provision reflects requests by many commenters from the securities industry that the rule permit this flexibility. We believe that broker-dealers, funds, and registered advisers should be able to combine initial, annual, or revised disclosures in one document and to give, on a collective basis, a consumer only one copy of the notice. For example, a clearing broker could provide a joint notice with an introducing broker for which it clears transactions on a fully disclosed basis, or a fund complex could provide a joint notice for all the funds in the complex. We emphasize that the notice must be accurate for each institution that uses the notice, and must identify each institution by name.[143]

B. Subpart B—Limits on Disclosure

Sections 248.10 through 248.12 of Regulation S–P contain limitations concerning (i) disclosure of nonpublic personal information to nonaffiliated third parties, (ii) redisclosure or reuse of information that a financial institution discloses to other parties, and (iii) sharing of account number information for marketing purposes.

Section 248.10 Limits on Disclosure of Nonpublic Personal Information to Nonaffiliated Third Parties

We are adopting the limits on disclosure of nonpublic personal information to nonaffiliated third parties, substantially as proposed.[144] 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 (i) provides the consumer with a notice of the institution's privacy policies and practices, (ii) provides the consumer with a clear and conspicuous notice that the consumer's nonpublic personal information may be disclosed to nonaffiliated third parties, (iii) gives the consumer an opportunity to opt out of that disclosure, and (iv) informs the consumer how to opt out.[145]

Most commenters on this section focused on the question of what is a reasonable opportunity to opt out. Some suggested that the rule permit a financial institution to begin sharing information immediately after it provides the opt out and initial notice in connection with an electronic transaction, such as an ATM transaction. Others advocated a mandatory delay of 120 days after the notices are provided.

We believe that the wide variety of suggestions underscores the appropriateness of a more general test rather than a mandatory waiting period in all cases. If a broker-dealer intends to disclose nonpublic personal information that it obtains through an isolated 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 broker-dealer to wait before sharing the information.[146] For notices that are provided by mail, however, we believe the consumer should have additional time. In these latter circumstances, we consider 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 after the date the opt out notice was mailed.[147] The final rule also provides an example of a reasonable opportunity for opting out in connection with accounts opened electronically.[148] However, we have not tried to anticipate every scenario and establish a specific period for each. Instead, the rule provides that the consumer must be given a reasonable opportunity to opt out and then includes some illustrative examples of what would be reasonable in different contexts.[149]

Section 248.11 Limits on Redisclosure and Reuse of Information

We are revising the limits on redisclosure and reuse to clarify their scope. The limits on redisclosure and reuse that apply to recipients of nonpublic personal information and their affiliates will depend on whether the information was provided under an exception in section 502(e) of the G–L–B Act.

Section 502(c) of the G–L–B Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution must not, directly or indirectly through an affiliate, disclose that information to

[140] *See* section 248.9(c)(1)(ii). A customer may request no communication or that the institution refrain from sending the annual notices. We note, however, that broker-dealers, funds, and registered advisers must provide customers with any communications (such as shareholder reports or confirmation statements) required under the federal securities laws. *See, e.g.,* 15 U.S.C. 80a–29(e). These institutions also must provide customers with initial, opt out, and revised privacy notices. *See* sections 248.4, 248.7, 248.8.

[141] *See* section 248.9(e)(2)(iii).

[142] *See* section 248.9(f). *See also* Proposing Release, *supra* note 4, at paragraph following n.34 (''[t]he proposed rules do not prohibit two or more institutions from providing a joint initial, annual, or opt out notice * * *'').

[143] Records concerning privacy notices delivered to consumers and consumer opt outs must be maintained in accordance with the recordkeeping requirements of 17 CFR 240.17a–4 (broker-dealers); 270.31a–2 (funds); 275.204–2 (registered advisers). *See also* section 248.30 (requiring broker-dealers, funds, and registered advisers to establish procedures and policies to safeguard customer information and records).

[144] Section 248.10.

[145] Proposed section 248.7 implemented these provisions by requiring a broker-dealer, fund, or registered adviser to give the consumer the initial notice required by section 248.4, the opt out notice required by section 248.8, and a reasonable opportunity to opt out.

[146] *See* section 248.10(a)(3)(iii).

[147] *See* section 248.10(a)(3)(i).

[148] *See* section 248.10(a)(3)(ii).

[149] Some commenters stated that the proposal inappropriately implied that the opportunity to opt out by mail is available only when a consumer has a customer relationship with the financial institution. *See* proposed section 248.7(a)(3)(i). The final rule deletes the reference to a customer relationship in that section to avoid creating that implication. *See* section 248.10(a)(3)(i).

any person that is not affiliated with the financial institution or the third party, unless the disclosure would be lawful if made directly by the financial institution. A broker-dealer, fund, or registered adviser generally may disclose nonpublic personal information to a nonaffiliated third party (i) for any purpose if the consumer has received a privacy and opt out notice and has not exercised the right to opt out, (ii) under section 502(b), and (iii) in accordance with specific enumerated exceptions under section 502(e).

The limits on redisclosure and reuse in the proposed rule reflected our belief that implicit in the joint marketing and enumerated exceptions is the idea that information may be used only for the purposes for which the third party received it.[150] The proposed rules implemented section 502(c) by imposing limits on redisclosure for a broker-dealer, fund, or registered adviser that receives information from a nonaffiliated financial institution, and for any nonaffiliated third party that receives nonpublic personal information from a broker-dealer, fund, or registered adviser.[151] The proposed rules also implemented the implicit limitations on reuse by imposing limits on the ability of broker-dealers, funds, and registered advisers and nonaffiliated third parties to reuse nonpublic personal information they receive.[152]

We sought comment on the correct interpretation of ''lawful'' 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 initially made the disclosure. Finally, we invited comment on whether the rules 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.

Limits on reuse and redisclosure. Commenters who disagreed with the proposal to impose limits on reuse argued 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. We disagree. Although section 502(c) does not expressly address reuse, reuse limitations are, as indicated, implicit in the provisions authorizing or permitting disclosures. For example, it would be inconsistent with the purposes of the Act to permit information disclosed in accordance with section 502(e)(1) (which permits disclosures as necessary to effect, administer, or enforce a transaction with a consumer or in connection with certain routine activities related to such a transaction) to be used for the third party recipient's marketing purposes. Moreover, permitting reuse without limits would undermine the protections afforded to a consumer who does not establish a customer relationship. Such a person does not receive notice that the disclosures under section 502(e) are even made because these disclosures do not entitle the consumer to any privacy or opt out notice. Thus, the limits on reuse are the only protection under the statute for a consumer who is not a customer. Accordingly, consistent with the purposes of the G–L–B Act, the rule limits the reuse of information received under an exception of the Act.[153]

By contrast, when a consumer decides not to opt out after receiving adequate notices and the opportunity to do so, that consumer has decided to permit the broker-dealer, fund, or registered adviser to share his or her nonpublic personal information with the categories of entities identified in the 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 G–L–B Act provides additional protection in section 502(c) by restricting a recipient's ability to redisclose information to entities not affiliated with either the recipient or the financial institution making the initial disclosure. Thus, if a consumer permits a broker-dealer, fund, or registered adviser 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 consistent with those notices.

Limits on redisclosure and reuse when information is received under section 502(e). If a broker-dealer, fund, or registered adviser *receives* nonpublic personal information provided under section 502(e), it may disclose the information to its affiliates or to the affiliates of the financial institution from which it received the information. The broker-dealer, fund, or registered adviser also may disclose and use the information under the same type of exceptions in the ordinary course of business to carry out the activity covered by the exception under which the institution received the information.[154] The affiliates of the broker-dealer, fund, or registered adviser may disclose and use the information, but only to the extent permissible for the broker-dealer, fund, or registered adviser.[155]

These same general rules apply to a third party other than a broker-dealer, fund, or registered adviser that receives nonpublic personal information from a broker-dealer, fund, or registered adviser. Thus, the third party receiving the information under one of the section 502(e) exceptions may disclose the information to its affiliates or to the affiliates of the broker-dealer, fund, or registered adviser that made the disclosure. The third party also may disclose and use the information under 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.

Limits on redisclosure and reuse when information is not received under section 502(e). If a broker-dealer, fund, or registered adviser receives nonpublic personal information *outside* one of the section 502(e) exceptions, it may disclose the information to (i) its affiliates, (ii) the affiliates of the financial institution that made the initial disclosure, or (iii) any other person if the disclosure would be lawful if made directly by the financial institution from which the information was received.[156] Thus, the receiving broker-dealer, fund, or registered adviser may disclose under one of the section 502(e) exceptions.

If a third party receives information from a broker-dealer, fund, or registered adviser outside one of the section 502(e) exceptions, the third party may disclose to its affiliates or to the affiliates of the broker-dealer, fund, or registered adviser. The third party also may disclose to any other person if the disclosure would be lawful if made by the broker-dealer, fund, or registered

[150] For example, as discussed further below in this section, permitted use for an enumerated exception would not include use for marketing purposes.

[151] *See* proposed section 248.12(a)(1), 248.12(b)(1).

[152] *See* proposed section 248.12(a)(2), 248.12(b)(2).

[153] *See* G–L–B Act § 504(a)(1) (authorizing the Commission to prescribe regulations necessary to carry out the purposes of Title V).

[154] *See* sections 248.14, 248.15.

[155] *See* section 248.11(a).

[156] The examples also provide that a broker-dealer, fund, or registered adviser may redisclose information according to the privacy notices of the institution making the initial disclosures, as limited by any opt out elections received by that institution. Section 248.11(b)(2).

adviser. The third party's affiliates may disclose and use the information to the same extent permissible for the third party.

If an entity receives information outside of one of the section 502(e) exceptions, that entity will in essence ''step into the shoes'' of the broker-dealer, fund, or registered adviser that made the initial disclosures. Thus, if the broker-dealer, fund, or registered adviser 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 comply with those representations. Otherwise, the subsequent disclosure by the receiving entity would not comply with the notices given to consumers and would not, therefore, be lawful. Even if these representations do not prevent the recipient from redisclosing the information, the recipient's ability to redisclose will be limited by whatever opt out instructions the consumer gave to the broker-dealer, fund, or registered adviser making the initial disclosures and by any new opt out instructions the consumer gives after the initial disclosure. The receiving entity, therefore, must have procedures in place to monitor continually the status of who opts out and to what extent. Given these practical limitations on the ability of a recipient to disclose under another institution's privacy and opt out notices, entities are most likely to redisclose under one of the section 502(e) exceptions (as implemented by sections 248.14 and 248.15 of the final rule).

Monitoring third parties. Most commenters stated that financial institutions should not have to monitor compliance with the redisclosure and reuse provisions of the rule, and we have decided not to revise the rule to impose a specific duty on broker-dealers, funds, and registered advisers to monitor third parties' use of nonpublic personal information they provide. The rule does not, however, address whether obligations to monitor reuse and redisclosure may arise in other contexts. Most of the commenters who requested that we not impose such a duty stated that they have contracts in place that limit the recipient's use of the information. In addition, the limits on reuse as stated in the final rule provide a basis for an enforcement action to be brought against an entity that violates those limits.[157]

Section 248.12 Limits on Sharing Account Number Information for Marketing Purposes

We are revising the proposed rule regarding limits on sharing account number information for marketing purposes[158] by (i) adding two exceptions that we believe are necessary to enable broker-dealers, funds, and registered advisers to engage in legitimate, routine business practices and that are unlikely to pose a significant potential for abuse, and (ii) clarifying that the prohibition does not apply in two circumstances frequently mentioned in the comments.[159] 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.'' The proposal applied this statutory prohibition to disclosures made directly or indirectly by a broker-dealer, fund, or registered adviser, and sought comment on whether the rule should include any exceptions to the prohibition. Some commenters suggested various exceptions while other commenters supported a flat prohibition in order to protect consumers from unscrupulous practices.

Disclosures to a financial institution's agent or service provider. Several financial institutions stated that they use agents or service providers to conduct marketing on the institution's behalf. This might occur, for example, when a broker-dealer instructs a service provider that assists in the delivery of required regulatory notices to include a ''statement stuffer'' about the broker-dealer's products and services. We recognize the need to disclose account numbers in this instance, and believe that this kind of disclosure poses little risk to the consumer.

Several commenters argued that the final rule should exclude disclosures to agents because they effectively act as the financial institution in marketing the financial products and services of the broker-dealer, fund, or registered adviser. We are concerned, however, that the agent of these financial institutions may engage in practices contrary to the institution's instructions. While a broker-dealer, fund, or registered adviser frequently will use agents to assist it in marketing its products, providing agents access to a consumer's account number may erode a consumer's protections. Accordingly, we have added an exception to permit a broker-dealer, fund, or registered adviser to disclose account numbers to an agent for the purpose of marketing the institution's financial product or services as long as the agent has no authority to initiate charges to the account.[160]

Encrypted numbers. Many commenters urged us to exercise our exemptive authority to permit the transmission of account numbers in encrypted form or to clarify that the prohibition applies only to disclosure to nonaffiliated third parties who are not subject to one of the exceptions under sections 248.13, 248.14, or 148.15. Several commenters noted that financial institutions frequently use encrypted account numbers and other internal identifiers of an account to ensure that a consumer's instructions are properly executed. The inability to continue using these internal identifiers would increase the likelihood of errors in processing a consumer's instructions. These commenters also noted that if internal identifiers are not used, a consumer would have to provide an account number in order to ensure proper handling of a request. This procedure could 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. One commenter also noted that customer account numbers are protected by strict contractual confidentiality provisions.

We believe an encrypted account number without the key is not the same as the number itself and thus falls outside the prohibition in section 502(d). The G–L–B Act focuses on numbers that provide *access* to an account. The encrypted number, however, operates as an identifier attached to an account for internal tracking purposes only, and without the key does not permit someone to access an account. For this reason the final rule clarifies 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.[161]

C. Subpart C—Exceptions

Sections 248.13 through 248.15 of Regulation S–P include exceptions from

[157] *See* section 248.11(c).

[158] *See* proposed section 248.13.

[159] *See* section 248.12.

[160] *See* section 248.12(b)(1).

[161] *See* section 248.12(c).

the provisions requiring financial institutions to provide privacy notices and opt out notices to consumers. These exceptions permit broker-dealers, funds, and registered advisers to disclose information to nonaffiliated third parties in circumstances such as maintaining or servicing a customer's account, or complying with federal, State, or local laws.

Section 248.13 Exception to Opt Out Requirements for Service Providers and Joint Marketing

We are adopting substantially as proposed an exception to the opt out requirements for service providers and joint marketing, with revisions to clarify the rule's scope.[162] Section 502(b) of the G–L–B Act permits financial institutions to share information with a nonaffiliated third party without providing the consumer a right to opt out if the third party is to perform services for (or functions on behalf of) the financial institution, including marketing the institution's own products or services, or financial products or services offered under a joint agreement between two or more financial institutions. Section 502(b)(2) requires the financial institution to ''fully disclose'' to the consumer that it will provide this information to the nonaffiliated third party before sharing the information and to enter 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 (i) will maintain the confidentiality of the information at least to the same extent as is required for the financial institution that discloses it, and (ii) will use the information solely for the purposes for which the information is disclosed or as otherwise permitted under the proposed rules.[163]

Commenters expressed concern that routine servicing agreements between a financial institution and, for instance, a customer account servicer would be subject to the requirements of the proposed rules.[164] These commenters noted that section 502(e) of the G–L–B Act contains several exceptions that permit broker-dealers, funds, and registered advisers to share information necessary to allow a third party to perform services for the institution. The commenters requested clarification that sharing information with a service provider under one of the section 502(e) exceptions is not subject to the requirements imposed under section 502(b)(2) of the G–L–B Act. We agree that when a broker-dealer, fund, or registered adviser is permitted to share nonpublic personal information with a nonaffiliated third party under section 502(e), the institution does not have to comply first with the requirements imposed by section 502(b)(2).

A few commenters also argued that it is illogical to impose requirements on service providers that receive information under section 502(b)(2) when no requirements are imposed on service providers that receive information under section 502(e). We believe, however, that a plain reading of section 502(b)(2) leads to that result.[165] We read the phrase ''if the financial institution fully discloses * * *'' as used in section 502(b)(2) to modify the phrase ''This 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, * * *.'' We therefore conclude 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).

The Proposing Release requested comment on whether the rule should include safeguards beyond those provided by the G–L–B Act to protect a financial institution from the risks that can arise from agreements with third parties. The majority of commenters who addressed the issue argued that the rule should not. We agree that the protections set out in the statute, as implemented by section 248.13(a)(1), are adequate for purposes of the privacy rules. Those protections require a financial institution to provide the initial notice required by section 248.4 as well as to enter into a contractual agreement with a third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the institution disclosed the information, including use under an exception in sections 248.14 or 248.15 in the ordinary course of business to carry out those purposes. These limitations will preclude recipients from sharing a consumer's nonpublic personal information through a chain of third party joint marketing agreements.

Many commenters recommended that the Commission permit broker-dealers, funds, and registered advisers to grandfather prior joint marketing and servicing agreements, or permit institutions to comply with the requirements by notifying existing service providers about the privacy rules' requirements. One commenter stated that without a grandfather provision, institutions would need more than six months to review prior agreements and negotiate amendments with third parties. We believe 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 provides that contracts entered into on or before July 1, 2000 must be brought into compliance with the provisions of section 248.13 by July 1, 2002.[166]

Section 248.14 Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions

We have revised the proposed exceptions to notice and opt out requirements for processing and servicing transactions[167] to include disclosures made in connection with (i) servicing or processing financial products or services requested by the consumer or (ii) maintaining or servicing a customer account.[168] 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 in connection with the administration, processing, servicing, and sale of a consumer's account. Proposed section 248.10 implemented those exceptions by restating them with only stylistic changes that were intended to make the exceptions easier to read. The Proposing Release noted that the exceptions set out in proposed sections 248.10 and 248.11 do not affect a financial institution's obligation to provide initial and annual notices of its privacy policies and practices.

We received many comments from broker-dealers, funds, and registered

[162] *See* proposed section 248.9, section 248.13.

[163] *See* proposed section 248.9, (a)(2). The exceptions were set forth in proposed sections 248.10 and 248.11.

[164] *See* section 248.13.

[165] The statute states, in relevant part, that section 502(b)— 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.

[166] Section 248.18(c).

[167] *See* proposed section 248.10.

[168] Section 248.14.

advisers noting that, by deleting the statutory phrase ''in connection with'' from the exceptions for information shared (i) to service or process a financial product or service requested by the consumer or (ii) to maintain or service a customer account, we narrowed the application of the exception. We did not intend this result, and have changed the final rule accordingly.[169]

Several other commenters requested that the final rule provide specific examples of situations that would fall within the exception for processing and servicing customer accounts (such as transfers from a broker-dealer to its registered representatives, or as necessary to arbitrate a dispute, with the consent of the consumer's fiduciary or representative). Others stated that certain services, such as those provided by attorneys, are ''necessary'' to effect, administer, or enforce a transaction. We believe 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, we have not listed specific types of disclosures in the regulation as necessarily falling within the scope of the exception because we are concerned that 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 in which a financial institution uses an agent to provide services to a consumer, that the consumer does not have to request directly or authorize the service provider to provide the financial product or service but may request it from the financial institution instead. For example, a consumer may ask the fund or its transfer agent for additional account information that the transfer agent provides as a service for the fund. We agree that the communication may be between the consumer and the service provider, and note that the rule governing agents as set out in the definition of ''consumer'' above provides the flexibility sought by the commenters. An individual will not be a consumer of an entity that is acting as agent for a broker-dealer, fund, or registered adviser in connection with that institution's providing a financial product or service to the consumer.

Section 248.15 Other Exceptions to Notice and Opt Out Requirements

We are adopting as proposed the section that includes ''other'' exceptions to the notice and opt out requirements. As noted above, section 502(e) of the G–L–B Act contains several exceptions to the requirements that otherwise would apply to the disclosures of nonpublic personal information to nonaffiliated third parties. The proposed rule set out those exceptions for disclosures that are not made in connection with the administration, processing, servicing, or sale of a consumer's account, and made stylistic changes to the statutory language that were intended to clarify the exceptions.[170] The proposal also provided an example of the consent exception in the context of a consumer who consents to having a broker or investment adviser confirm the amount of assets in the customer's account to a nonaffiliated mortgage lender so that the lender can evaluate the customer's application for a loan. We invited comment on whether we should add safeguards 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 consumer 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. Some commenters favored the additional safeguards discussed in the proposal, while others maintained that safeguards 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 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.

We have declined to elaborate on the requirements for obtaining consent or the consumer safeguards that should be in place when a consumer consents. We believe that the resolution of this issue is appropriately left to the particular circumstances of a given transaction. We note that any broker-dealer, fund, or registered adviser 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 institution and the consumer. We also note that a consumer may always revoke his or her consent. In light of the safeguards already in place, we have decided not to adopt additional safeguards in the consent exception.

Many commenters offered specific suggestions for additional exceptions or revisions to the proposed exceptions. In some cases, the suggestions are accommodated elsewhere in the regulation (such as exceptions to permit disclosures to independent contractor registered representatives or attorneys to effect a transaction).[171] In other cases, the suggestions are inconsistent with the statute.[172] Accordingly, we have retained the statement of the exceptions as proposed.[173]

D. Subpart D—Relation to Other Laws; Effective Date

Sections 248.16 through 248.18 of Regulation S–P include provisions that explain the interaction between the regulation and certain other laws, and that provide an effective date and compliance date for the regulation.

Section 248.16 Protection of Fair Credit Reporting Act

We are adopting as proposed the section that explains the interaction between Regulation S–P and the Fair Credit Reporting Act.[174] 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 Banking Agencies' regular examination authority. Paragraph (c) of section 506 states that, except for these amendments to the FCRA, 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 section 248.14 implemented section 506(c) of the G–L–B Act by restating the statute,

[169] *See* section 248.14(a).

[170] Proposed section 248.11.

[171] *See* section 248.14(a) (excepting from initial and opt out notice requirements disclosures to nonaffiliated third parties as necessary to effect a transaction that a consumer requests or in connection with servicing or processing a financial product that a consumer requests or authorizes).

[172] One commenter, for example, suggested that the rule completely exempt a financial institution from all of the requirements under Title V if the institution makes no disclosures other than those permitted by section 502(e).

[173] *See* section 248.15.

[174] Section 248.16.

making only minor stylistic changes intended to make the rule clearer.

Comments about this provision focused 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 section 248.6, above, we do not believe that the annual disclosure mandated by the G–L–B Act affects in any way the obligations imposed by the FCRA.

Section 248.17 Relation to State laws.

We are adopting as proposed the section that explains the interaction between Regulation S–P and State laws.[175] Section 507 of the G–L–B Act provides 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 Federal Trade Commission (''FTC'') after consultation with the agency that regulates either the party filing a complaint or the financial institution about whom the complaint was filed, and may be initiated by any interested party or on the FTC's own motion. The proposed rule essentially restated section 507, stating that the proposed rules (as opposed to the statute) do not preempt State laws that provide greater protection for consumers than do the rules.

Commenters on this section expressed concern about the potential differences between federal and State privacy laws. Several supported coordination and cooperation among federal and State regulators to ensure consistency in privacy policies. Some commenters requested clarification of whether a particular State law would be considered more restrictive, while others suggested that the final rules establish a choice of law principle for financial institutions operating in more than one State. These and other suggestions made by the commenters appear to exceed the scope of this rulemaking.

Section 248.18 Effective Date; Transition Rule

We are adopting as proposed the effective date for Regulation S–P of November 13, 2000, and are providing a compliance date of July 1, 2001.[176] We also are adding a provision that clarifies the requirement that financial institutions provide initial privacy and opt out notices to customers by July 1, 2001, and a provision that phases in compliance with respect to existing service agreements.[177]

Section 510 of the G–L–B Act states that, as a general rule, the relevant provisions of Title V take effect six months after the date on which rules are required to be adopted, *i.e.,* November 12, 2000. However, section 510(1) authorizes us to prescribe a later date in the rules adopted under section 504. The Proposing Release sought comment on the effective date prescribed by the statute.[178] 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 Proposing Release 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.[179]

The Congressional Privacy Caucus, several members of Congress, and other commenters have urged the Commission and the Agencies not to delay the effective date past the date set forth in the G–L–B Act.[180] By contrast, the overwhelming majority of commenters from the securities industry who addressed 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, and creating management oversight systems. Several commenters suggested that it would be less effective and potentially more confusing for consumers to receive several notices 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. Requests for extensions of the effective date typically ranged from six to 24 months from the proposed effective date of the rule (*i.e.,* from November 13, 2000).

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.

We agree that six months may be insufficient in certain instances for a financial institution to have ensured that its forms, systems, and procedures comply with the rule. In order to accommodate situations requiring additional time, we 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. Given that this provides financial institutions more than 12 months in which to comply with the rules, we have determined that 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. We believe that 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.

We encourage financial institutions to provide disclosures as soon as practicable. Broker-dealers, funds, and registered agents that do not disclose nonpublic personal information to third parties have fewer burdens under the regulation (both in terms of the notice requirements and opt out mechanism) and should therefore be able to provide privacy notices to their consumers sooner. 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 or account statements to consumers in the first quarter of 2001 to increase the likelihood that a consumer will not mistake the notices for an unwanted solicitation.

[175] Section 248.17.

[176] Section 248.18(a).

[177] Section 248.18(b), (c).

[178] Because Nobvember 12, 2000 is a Sunday, the proposed rule provided an effective date of Monday, November 13, 2000. *See* proposed rule 248.16(a).

[179] *See* Proposing Release, *supra* note 4, at discussion of proposed section 248.16.

[180] *See supra* note 6.

The extension of the compliance date should provide 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 rules is avoided. Accordingly, we have not adopted the suggestion that initial notices be required only for new customers after the effective date of the rule.

Broker-dealers, funds, and registered advisers need not give initial notices to customers whose relationships have terminated before the date by which institutions must be in compliance with the rules. 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 broker-dealer, fund, or registered adviser would have to provide a privacy and opt out notice to them if the institution intended to disclose their nonpublic personal information to nonaffiliated third parties beyond the exceptions in sections 248.14 and 248.15.

Full compliance with the rules' restrictions on disclosures is required on July 1, 2001. To be in full compliance, broker-dealers, funds, and registered advisers must have provided their existing customers with a privacy notice, an opt out notice, and a reasonable amount of time to opt out before that date. If these have not been provided, the disclosure restrictions will apply. This means that a broker-dealer, fund, or registered adviser would have to cease sharing customers' nonpublic personal information with nonaffiliated third parties on that date, unless it may share the information under an exception under sections 248.14 or 248.15. Broker-dealers, funds, and registered advisers that both provide the required notices and allow a reasonable period of time to opt out before July 1, 2001, may continue to share nonpublic personal information after that date for customers who do not opt out.

E. Subpart E—Safeguard Procedures

Section 248.30 Procedures To Safeguard Customer Information and Records

Commenters on this section supported the proposal, and we are adopting this section as proposed. Section 501 of the G–L–B Act directs the Commission (and the Agencies) to establish appropriate standards for financial institutions relating to administrative, technical, and physical safeguards to protect customer records and information. The rules implement this section by requiring every broker-dealer, fund, and registered adviser to adopt policies and procedures to address the safeguards described above. Consistent with the Act, the proposed rule further requires that the policies and procedures be reasonably designed to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Some commenters recommended that the Commission add an example to clarify that various financial institutions in a fund complex could satisfy the rule by adopting a single set of policies and procedures for the fund complex. We believe that a single set of policies and procedures for a fund complex could satisfy the rule's requirements, as long as those policies and procedures have been determined to be appropriate for each institution to which they apply.

IV. Appendix—Sample Clauses

In order to provide additional guidance to broker-dealers, funds, and registered advisers concerning the level of detail we believe is appropriate under the Act, we have prepared a variety of sample clauses for institutions to consider. We urge broker-dealers, funds, and registered advisers to carefully review whether these clauses accurately reflect a given institution's policies and practices before using the clauses. Broker-dealers, funds, and registered advisers are free to use different language and to include additional detail as they think is appropriate in their notices.

V. Comparison Chart

Below is a chart showing the comparison of the sections in the final privacy rules and 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	9(d)
4(d)(4) ..	Retainable notice	9(e)
N/A	Joint relationships (privacy notice).	9(g)
5(b)	How to provide annual notice.	9(a)
5(b)	Actual notice of annual notice.	9(c)
5(c)	Terminated customer relationships.	5(b)
N/A	Delivering short-form initial notices.	6(d)
7	Main operative provision.	10
8(a)	Opt out methods and opt out notice content.	7(a)
8(b)(1) ..	How to deliver opt out notices.	9(a)
8(b)(2) ..	Oral delivery	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) & (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

VI. Guidance for Certain Institutions

To minimize the burden and costs to a broker-dealer, fund, or registered adviser (''you'') and generally clarify the operation of the final rules, we have included this guidance that you may use in conjunction with the sample clauses in the Appendix. 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 sections 248.14 or 248.15, 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 sections 248.14 and 248.15.[181]

In addition, if you disclose nonpublic personal information in accordance with the exception in section 248.13 (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 privacy 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 section 248.4(c). In general, an individual who opens a brokerage account or enters into an investment advisory contract (whether written or oral) with you is your customer. By contrast, an individual who establishes an account solely for the purpose of liquidating or purchasing securities as an accommodation, *i.e.,* on a one-time basis, without the expectation of engaging in other transactions, is not your customer. 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 (section 248.4(a)(1)). For example, you must provide a privacy notice to an individual not later than when that individual opens a brokerage account or purchases fund shares in his or her own name. Thus, you can provide the notice to a brokerage account customer together with the account agreement or to a fund shareholder with the application to purchase shares.

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 (section 248.4(d)) if the earlier notice covered the subsequent product.

For instance, if Alison Individual walks into Broker-Dealer for the first time on July 2, 2001, to open a cash account, then Broker-Dealer complies with section 248.4(a)(1) of the rules if it provides an initial notice to Alison together with the account agreement. When Alison opens her cash account, she becomes a customer of Broker-Dealer. Alison maintains her cash account and, six months later, returns to the Broker-Dealer to open a margin account. If the initial notice that the Broker-Dealer provided to Alison was accurate with respect to the margin account, then the Broker-Dealer need not provide another initial notice to her when she opens the margin account because it has provided a notice to Alison that covered the margin account when she opened her cash account.

C. *Method of providing the initial notice.* You must provide your initial notice so that each customer can reasonably be expected to receive it (section 248.9(a)). For example, you may provide the initial notice by mailing a printed copy of it together with a prospectus. Similarly, you may provide the initial notice by hand-delivering a printed copy of it to the customer together with a brokerage account application or an investment advisory contract.

D. *Compliance with initial notice requirement for existing customers by compliance date.* You must provide an initial notice to each of your current customers not later than July 1, 2001 (section 248.18(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 section 248.5(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. You do not need to provide an annual notice in addition to an initial notice in the same 12-month period.

For example, assume that Broker-Dealer 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 opens a cash account with Broker-Dealer on July 2, 2001, thereby becoming a customer, then Broker-Dealer must provide an initial notice to Alison together with the account agreement or earlier. Broker-Dealer must provide an annual notice to Alison by December 31, 2002. If Broker-Dealer 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 (section 248.9(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 (section 248.9(g)).

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

- The categories of nonpublic personal information that you collect (section 248.6(a)(1));
- The fact that you do not disclose nonpublic personal information about your current and former customers to affiliates or nonaffiliated third parties, except as authorized by sections 248.14 and 248.15 (section 248.6(a)(2)–(4)). 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 (section 248.6(c));
- Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (section 248.6(a)(8)).

For each of these items of information above, you may use a sample clause from the Appendix.

Note: You may use a sample clause only if that clause accurately describes your actual policies and practices.

I. *Example of notice.* If Broker-Dealer (i) does not have any affiliates and (ii) only discloses nonpublic personal information to nonaffiliated third parties as authorized under sections 248.14 and 248.15, Broker-Dealer may comply with the requirements of section 248.6 of the rules by using the following notice, if applicable.

Broker-Dealer 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*

[181] 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 rules, notably sections 248.7, 248.8, and 248.13, 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 rules, notably section 248.6(a)(7), as applicable.

• *Information we receive from a consumer reporting agency.*[182]

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

If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

Broker-Dealer restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. Broker-Dealer maintains physical, electronic, and procedural safeguards to guard your nonpublic personal information.

J. *Initial and annual notices must be clear and conspicuous.* We emphasize that you must ensure that both the initial and annual notices are clear and conspicuous, as defined in section 248.3(c).

K. *Example of notice for disclosure to service providers and joint marketers.* If you disclose nonpublic personal information in accordance with the exception in section 248.13, for service providers and joint marketers, you also must include an accurate description of that information. You may comply with the requirements of section 248.13 of the rules 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.

L. *Internal controls/supervision.* The Commission expects brokers-dealers, funds, and registered advisers to create appropriate internal control systems and exercise appropriate supervision over compliance with this rule. Compliance systems could include the maintenance of copies of the notices provided to consumers and customers, documentation in customer files showing compliance, and procedures for handling and monitoring opt out requests.

VII. Cost-Benefit Analysis

The Commission is sensitive to the costs and benefits that result from its rules and understands that the rules may impose costs on broker-dealers, funds, and registered advisers. Nevertheless, the rules implement the privacy provisions of Title V and, we believe, impose no costs in addition to those that would result from compliance with the G–L–B Act.

We believe that the requirements to provide opt out notices and to protect customer information will benefit consumers and customers by protecting the privacy of their nonpublic personal information. In addition, the requirements to provide initial and annual privacy notices will allow customers to compare the privacy policies of financial institutions.

We also believe that the rules provide greater certainty to the private sector on how to comply with the G–L–B Act because they are consistent with and comparable to the rules adopted by the Agencies. The examples in the rules and the sample clauses in the Appendix also should provide guidance on how the rules will be enforced with respect to broker-dealers, funds, and registered advisers. Finally, in order to reduce compliance burdens, the rules allow broker-dealers, funds, and registered advisers flexibility to distribute notices and to adopt policies and procedures to protect customer information that are best suited to the institution's business and needs. These benefits are difficult to quantify, and we received no data from commenters.

We estimate that approximately 5500 broker-dealers, 4300 funds, and 8100 registered advisers will be required to comply with the rules. In the first year after the rules are adopted, these institutions must comply with the following requirements: (i) Prepare notices describing the institution's privacy policies; (ii) provide an initial privacy notice and opt out notice to each consumer; (iii) provide an initial privacy notice to each new customer (who did not receive a notice when he or she was a consumer); (iv) provide an annual privacy notice to each existing customer; (v) adopt policies and procedures that address the protection of customer information and records. After the first year, broker-dealers, funds, and registered advisers would be required to revise notices only to reflect changes in their privacy policies. Similarly, these institutions would have to revise their policies and procedures on safeguarding customer information as appropriate to ensure the protection of the information.

In the Proposing Release, we estimated certain costs of complying with the proposed rules.[183] We estimated that a registered adviser would spend on average $615 to draft a privacy notice,[184] and a broker-dealer or fund would spend on average $4920 to draft a privacy notice.[185] Therefore, we estimated a one-time cost to the industry of approximately $53.2 million to draft privacy notices.[186] For mailing the notices, we estimated that it would cost broker-dealers, funds, and registered advisers $2.6 million to provide to their customers initial notices in the first year after adoption, and the same amount to provide annual notices to customers each year after that.[187] In addition, we assumed that most broker-dealers, funds, and

[182] You need to describe only 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.

[183] *See* Proposing Release, *supra* note 4, at section IV.

[184] For purposes of the Paperwork Reduction Act, Commission staff has estimated that an investment adviser would require 4 hours of professional time (at $150 per hour) and 1 hour of clerical or administrative time (at $15 per hour) to prepare (or revise) its privacy notice, for a total of $615 ((4 × $150) + (1 × $15) = $615).

[185] For purposes of the Paperwork Reduction Act, Commission staff has estimated that a broker-dealer or investment company would require 32 hours of professional time and 8 hours of clerical or administrative time to prepare (or revise) its privacy notice, for a total of $4920 ((32 × $150) + (8 × $15) = $4920).

[186] This amount equals the sum of the costs for broker-dealers, funds, and registered advisers ((5500 + 4300) × $4920) + (8,100 × $615) = $53.2 million. The amount of time required for each institution to prepare (or revise) its privacy notices will vary depending on the extent to which (i) the institution shares information and (ii) the institution's sharing policy differs for certain consumers or customers. An institution that does not share information with affiliates or nonaffiliated third parties may provide a simplified notice. *See* section 248.6(c)(5). An institution that has many affiliates and has different policies on sharing based on the affiliate or the customer is likely to require much more time to draft its notices. Our estimate was based on the assumption that most broker-dealers and funds share nonpublic personal information about consumers or customers with their affiliates (or as permitted under one of the exceptions discussed above), but many fewer share information with nonaffiliated third parties, and that registered advisers generally do not share with affiliates or nonaffiliated third parties. For purposes of the Paperwork Reduction Act, Commission staff has estimated that a registered adviser would require, on average, about 5 hours, and a broker-dealer or fund would require from 5 to over 100 hours, with an average of about 40 hours, to prepare (or revise) its privacy notice.

[187] We assumed that broker-dealers, funds, and registered advisers generally would include the initial privacy notices to customers with disclosure documents or account statements that customers currently receive, and that the statements generally would be assembled and sent by organizations that specialize in mailing and distribution. The individual cost per institution would vary significantly depending on the number of the institution's customers. The estimate was based on an average additional cost per mailing of $0.02 for 130.7 million investor accounts. We assumed there are 53 million brokerage accounts, 77.3 million individual fund shareholders (*see* Investment Company Institute, 1999 Mutual Fund Fact Book 41 (May 1999)), and 400,000 customers of registered advisers. We noted that the estimated number of accounts may be significantly higher than the actual number because we were unable to estimate the number of individual accounts used for personal, family, or household purposes.

registered advisers currently have in place procedures to protect customer information. Thus, we estimated that each institution would on average require approximately 30 hours to review and revise its policies and procedures, with a one-time cost to the industry to comply with the rules of approximately $80.6 million.[188]

We received two comments on the cost-benefit analysis, both of which opined that we underestimated the costs and burdens of complying with Regulation S–P. One commenter suggested that we increase our estimate of the cost to mail annual notices to reflect the cost of providing revised privacy notices.[189] This commenter suggested that the cost for privacy notices would increase annual mailing costs by approximately $1.3 million per year.[190]

These commenters further noted that our estimates did not address other costs of compliance, including: Modifying existing systems and databases, developing new systems to track delivery of privacy notices and (if necessary) opt out elections, and training personnel. One commenter estimated that the overall cost of implementing the rules for a large firm would be at least $1 million. The other commenter provided no estimates for these additional costs. Neither commenter provided any specific data to explain the amount of time or the costs associated with the time they believe will be required to implement the rules.

The cost of developing and maintaining records of delivery of privacy notices and opt out elections, and costs for personnel training will vary greatly depending upon the size of the financial institution, its customer base, number of affiliates, and the extent to which the institution intends to share information. We have been unable to obtain any reliable information with which to quantify the amount of these costs. We recognize that the costs for a large institution that shares information with affiliates and nonaffiliated third parties and that has many customers may exceed $1 million, and that this could increase the compliance costs of the rules. We also believe that the costs for a small institution, such as a registered adviser, that has far fewer customers and does not share with affiliates or nonaffiliated third parties will be significantly less.

As discussed above, the privacy notices will allow customers of broker-dealers, funds, and registered advisers to compare the privacy policies of different institutions. This information is likely to result in some customers moving their accounts or relationships from one institution to another whose policies are better suited to the customers' needs. We are unable to estimate the number of customers who may make this transfer or the resulting economic impact on the industry. We do not believe, however, that customers would move their accounts from broker-dealers, funds, or investment advisers to a different type of financial institution (such as a bank), because we have no basis for assuming that the privacy policies adopted by 17,900 broker-dealers, investment companies, and registered investment advisers would not be sufficiently varied to address the needs of any customer.

VIII. Paperwork Reduction Act

Certain provisions of the rules contain ''collection of information'' requirements within the meaning of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520). The Commission published notice soliciting comments on the collection of information requirements in the Proposing Release,[191] and submitted these requirements to the Office of Management and Budget (''OMB'') for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. OMB approved the regulation's information collection requirements.[192] An agency may not conduct or sponsor, and a person is not required to respond to, an information collection unless it displays a currently valid OMB control number.[193]

IX. Summary of Final Regulatory Flexibility Analysis

The Commission has prepared a Final Regulatory Flexibility Analysis (''FRFA'' or ''analysis'') for Regulation S–P in accordance with 5 U.S.C. 604. The following summarizes the FRFA. A copy of the FRFA may be obtained by contacting Penelope W. Saltzman, Securities and Exchange Commission, 450 5th Street, NW., Washington, DC 20549–0506.

The analysis explains that Regulation S–P implements provisions of Title V and that, in general, Title V requires financial institutions to provide notice to consumers about the institution's privacy policies and practices. The statute also restricts the ability of a financial institution to share nonpublic personal information about consumers with nonaffiliated third parties, and allows consumers to prevent the institution from sharing nonpublic personal information about them with certain nonaffiliated third parties by ''opting out'' of the information sharing. In addition, Title V requires the Commission to establish appropriate standards for financial institutions subject to their jurisdiction to safeguard customer information and records.

Section 504 of the G–L–B Act authorizes the Commission and the Agencies to prescribe ''such regulations as may be necessary'' to carry out the purposes of Title V. As discussed in the analysis, we believe that by adopting rules implementing Title V that are consistent with and comparable to those of the Agencies, we will provide the private sector greater certainty on how to comply with the statute and clearer guidance on how the rules will be enforced with respect to the financial institutions subject to Title V that are under the Commission's jurisdiction.

The analysis states that the Proposing Release solicited comments on the IRFA, but we received none. Several commenters who addressed the proposed rules, however, suggested that the Commission reduce compliance burdens by, among other things, providing model forms, providing additional examples, adding additional flexibility for providing the initial notice, and extending the effective date. In response to these comments, we have

[188] The estimate represented the costs of 30 hours of professional time (at $150 per hour) ((5500 + 4300 + 8100) × 30 × $150 = $80.6 million). Our estimates were based on staff conversations with representatives from the industry. We understand that many large institutions currently have comprehensive policies and procedures for protecting customer information and records. Although the policies of those institutions may need little revision, there may be many departments or other divisions that will participate in the review. Smaller institutions that need less comprehensive policies may devote more time to implementation or revision of their policies and procedures.

[189] *See* section 248.8.

[190] This estimate was based on a cost of $0.02 per mailing to 130.7 million accounts every other year ($0.02 × 130.7 × 5 = $1.3 million). One commenter stated that it would cost $0.40 per piece to mail the privacy notices, the same cost as mailing a confirmation statement. We believe that this commenter assumed that it would have to provide a privacy notice to its existing customers in a separate mailing (as a confirmation must be sent). The extended compliance date should permit broker-dealers, funds, and registered advisers to mail privacy notices to existing customers together with another mailing, such as an account statement or shareholder report, so that the costs will be significantly reduced. The other commenter used our estimate of $0.02 in its estimate of mailing costs, and we have continued to use that estimate in our final cost-benefit analysis.

[191] *See* Proposing Release, *supra* note 4, at section V.

[192] The title for the collections of information is: ''Regulation S–P.'' The OMB control number for Regulation S–P is 3235–0537 (expiration date April 30, 2003).

[193] 44 U.S.C. 3506(c)(1)(B)(v).

provided a guide to assist broker-dealers, funds, and registered advisers in complying with the rules. The rules also include an Appendix with sample clauses that could be used in privacy notices under appropriate circumstances, and should be of particular help to small entities. Other revisions to the rules include: (i) A compliance date of July 1, 2001 (to allow more time to comply and more opportunity to include initial notices with other mailings); (ii) an example that permits householding annual privacy notices with prospectuses or investor reports delivered under the Commission's householding rules;[194] and (iii) permitting delivery of an initial notice within a reasonable time after establishing the customer relationship in two additional circumstances.[195]

As explained in the analysis, the rules will affect all broker-dealers, funds, and registered advisers, including small entities.[196] We estimate that approximately 1000 out of 5500 broker-dealers, 227 out of 4300 funds, and 1500 out of 8100 registered advisers are small entities.

The analysis explains that subject to certain exceptions, the rules generally require that a financial institution provide all of its *customers* the following notices: (i) An initial privacy notice (not later than when the customer relationship is established or, by July 1, 2001 for individuals who are your customers on that date); (ii) an opt out notice (before sharing the customer's nonpublic personal information with nonaffiliated third parties); and (iii) an annual privacy notice for the duration of the customer relationship.

The rules also require a financial institution to provide its *consumers* an initial privacy notice and an opt out notice prior to disclosing the individual's nonpublic personal information with nonaffiliated third parties. If the institution does not intend to share that information about its consumers, then it need not provide them with a privacy or opt out notice.

The many exceptions to the general rules stated above are set forth in sections 248.13, 248.14, and 248.15. The analysis notes that in cases in which a financial institution enters into a contract with a nonaffiliated third party to undertake joint marketing or to have the third party perform certain functions on behalf of the institution, no opt out notice need be given. In those cases, the institution must disclose to the consumer that it is providing the information and enter into a contract with the third party that restricts the third party's use of the information and requires the third party to maintain confidentiality of the information.

As discussed in the analysis, compliance requirements will vary depending, for example, on an institution's information sharing practices, whether the institution already has or discloses a privacy policy, and whether the institution already has established an opt out mechanism. A financial institution would have to summarize its practices regarding its collection, sharing, and safeguarding of certain nonpublic personal information in its initial and annual notices. However, if the institution does not share that information (or shares only to the extent permitted under the exceptions), its privacy notice may be brief. We believe that many financial institutions already have privacy policies in place as part of usual and customary business practices, and that many broker-dealers, funds, and investment advisers currently do not share nonpublic personal information about consumers with nonaffiliated third parties except as would be consistent with one of the many exceptions in the rules.[197] In the Proposing Release, we estimated that a registered adviser would spend an average of 5 hours to prepare a privacy notice, and a broker-dealer or fund would spend approximately 40 hours on average to prepare a privacy notice. We further understand that those institutions that do share information under one of the permitted exceptions generally have contract provisions that prohibit the third party's use of the information for purposes other than the purpose for which the information was shared. Thus we believe that, as a result of the rules, many financial institutions will not have to provide opt out notices to consumers, will have brief annual privacy notices for customers, and will not need to revise their contracts with nonaffiliated third parties to restrict those parties' use of information.

To minimize the burden and costs of distributing privacy policies, the rules do not specify the method for distributing required notices. As discussed more fully in the analysis, a financial institution may include an initial privacy statement with other required disclosure statements, and may include an annual notice with periodic account statements. We estimate that the costs of distributing the notices will be minimal because an institution will include the notices in mailings or distributions that it already sends to consumers and customers.

The analysis explains that the rules require every broker-dealer, fund, and registered adviser to adopt policies and procedures reasonably designed to safeguard customer records and information. The IRFA noted, and we continue to believe, that most if not all financial institutions already have policies and procedures to address the safety and confidentiality of consumer records and information. Nevertheless, financial institutions may review and revise their policies after the rules are adopted. The amount of time an institution will spend reviewing and revising its policies will depend, among other things, on the institution's current policies and its sharing practices. The rules do not specify the means by which institutions must ensure the safety of customer information and records in order to allow each institution to tailor its policies and procedures to its own systems of information gathering and transfer, and the needs of its customers. As noted in the IRFA, Commission staff estimated that in the first year after the rules are adopted, a financial institution would spend an average of 30 hours to adopt or revise its policies.

Two commenters argued that we underestimated the costs of implementing Regulation S–P. As explained in the analysis, the commenters did not provide estimates of the amount of time or the costs to implement the rules. We have been unable to obtain reliable information regarding these costs. Therefore, we have not provided an estimate of the cost of implementing the rules for

[194] *See* section 248.9(c)(2).

[195] *See* section 248.4(e)(1)(ii) and (iii).

[196] For purposes of the Regulatory Flexibility Act, under the Exchange Act a small entity is a broker or dealer that (i) had total capital of less than $500,000 on the date in its prior fiscal year as of which its audited financial statements were prepared or, if not required to file audited financial statements, on the last business day of its prior fiscal year, and (ii) is not affiliated with any person that is not a small entity and is not affiliated with any person that is not a small entity. 17 CFR 240.0–10. Under the Investment Company Act a ''small entity'' is an investment company that, together with other investment companies in the same group of related investment companies, has net assets of $50 million or less as of the end of its most recent fiscal year. 17 CFR 270.0–10. Under the Investment Advisers Act, a small entity is an investment adviser that ''(i) manages less than $25 million in assets, (ii) has total assets of less than $5 million on the last day of its most recent fiscal year, and (iii) does not control, is not controlled by, and is not under common control with another investment adviser that manages $25 million or more in assets, or any person that had total assets of $5 million or more on the last day of the most recent fiscal year. 17 CFR 275.0–7.

[197] For example, as noted in the Proposing Release, investment advisers have fiduciary duties under state law that limit their ability to share information with third parties. *See* Proposing Release, *supra* note 4, at n.4. This and other assumptions discussed in this section also are based on staff conversations with representatives from the securities industry.

individual institutions or for the industry as a whole. Although we recognize that the cost of implementing the rules may be $1 million or more for a large institution that shares information with affiliates and nonaffiliated third parties, we believe the costs for small institutions that do not share nonpublic personal information about consumers will be substantially less.

The analysis explains that the Regulatory Flexibility Act directs the Commission to consider significant alternatives that would accomplish the stated objective, while minimizing any significant adverse impact on small entities. As noted above, we believe that a number of revisions made to the final rules will benefit small entities. Finally, the analysis notes that the rules contain performance rather than design standards. The rules do not specify the (i) form of privacy notices, (ii) method of delivery of the notices to customers and consumers, or (iii) policies and procedures that broker-dealers, funds, and registered advisers must adopt to ensure the privacy of the financial information and records of their customers and consumers. Therefore, the rules provide these entities substantial flexibility that allows them to meet the requirements of Regulation S–P in a way that best suits the institution's individual needs.

X. Analysis of Effects on Efficiency, Competition, and Capital Formation

Section 23(a)(2) of the Exchange Act [198] requires the Commission, in adopting rules under the Exchange Act, to consider the anti-competitive effects of any rules it adopts. The rules, which implement Title V, apply to all broker-dealers, funds, and registered advisers. Each of these institutions must provide initial and annual privacy notices to customers as well as initial notices and opt out forms to consumers before the institution shares nonpublic personal information about consumers with nonaffiliated third parties. These institutions also must establish standards for protecting customer information and records.

Other financial institutions will be subject to substantially similar privacy notice and opt out requirements under rules adopted by the Agencies.[199] Under the G–L–B Act, these agencies also are required to adopt rules addressing policies and procedures for protecting customer information.[200] Therefore, all financial institutions will have to bear the costs of implementing the rules or substantially similar rules.

The rules do not dictate the privacy policies of any financial institution. Some customers may move their accounts from one institution to another based on the institution's privacy policies. Thus, the rules may promote competition among financial institutions based on customers' preferences regarding privacy policies.

Section 3(f) of the Exchange Act [201] and section 2(c) of the Investment Company Act [202] require the Commission, when engaging in rulemaking that requires it to consider or determine whether an action is necessary or appropriate in the public interest, to consider whether the action will promote efficiency, competition, and capital formation. We solicited comment on these matters in connection with the proposed rules but received no comment.[203] Our analysis on competition is discussed above. The rules will result in additional costs for financial institutions, which may affect the efficiency of these institutions. On the other hand, the rules will allow customers of financial institutions to compare privacy policies, which may result in customers choosing to do business with a financial institution based on its policies. We are not aware of any effect the rules will have on capital formation.

XI. Statutory Authority

The Commission is adopting Regulation S–P under the authority set forth in section 504 of the G–L–B Act [15 U.S.C. 6804], sections 17 and 23 of the Exchange Act [15 U.S.C. 78q, 78w], sections 31 and 38 of the Investment Company Act [15 U.S.C. 80a–30(a), 80a–37], and sections 204 and 211 of the Investment Advisers Act [15 U.S.C. 80b–4, 80b–11].

Text of Rules

List of Subjects in 17 CFR Part 248

Brokers, Dealers, Investment advisers, Investment companies, Privacy, Reporting and recordkeeping requirements.

For the reasons set out in the preamble, the Commission amends Title 17, Chapter II of the Code of Federal Regulations by adding a new part 248 to read as follows:

PART 248—REGULATION S–P: PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

Authority: 15 U.S.C. 6801–6809; 15 U.S.C. 78q, 78w, 80a–30(a), 80a–37, 80b–4, and 80b–11.

§ 248.1 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 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

[198] 15 U.S.C. 78w(a)(2).

[199] *See, e.g.*, Banking Agencies' Release, *supra* note 2.

[200] G–L–B Act § 501(b).

[201] 15 U.S.C. 78c(f).

[202] 15 U.S.C. 80a–2(c).

[203] *See* Proposing Release, *supra* note 4, at section VII.

out'' of that disclosure, subject to the exceptions in §§ 248.13, 248.14, and 248.15.

(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 primarily for business, commercial, or agricultural purposes. This part applies to brokers, dealers, and investment companies, as well as to investment advisers that are registered with the Commission. It also applies to foreign (non-resident) brokers, dealers, investment companies and investment advisers that are registered with the Commission. These entities are referred to in this part as ''you.'' This part does not apply to foreign (non-resident) brokers, dealers, investment companies and investment advisers that are not registered with the Commission. 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).

§ 248.2 Rule of construction.

The examples in this part and the sample clauses in appendix A of this part provide guidance concerning the rule's application in ordinary circumstances. The facts and circumstances of each individual situation, however, will determine whether compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this part.

§ 248.3 Definitions.

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

(a) *Affiliate* of a broker, dealer, or investment company, or an investment adviser registered with the Commission means any company that controls, is controlled by, or is under common control with the broker, dealer, or investment company, or investment adviser registered with the Commission. In addition, a broker, dealer, or investment company, or an investment adviser registered with the Commission will be deemed an affiliate of a company for purposes of this part if:

(1) That company is regulated under Title V of the G–L–B Act by the Federal Trade Commission or by a Federal functional regulator other than the Commission; and

(2) Rules adopted by the Federal Trade Commission or another federal functional regulator under Title V of the G–L–B Act treat the broker, dealer, or investment company, or investment adviser registered with the Commission as an affiliate of that company.

(b) *Broker* has the same meaning as in section 3(a)(4) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(4)).

(c)(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) 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.

(d) *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.

(e) *Commission* means the Securities and Exchange Commission.

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

(g)(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 is your consumer if he or she provides nonpublic personal information to you in connection with obtaining or seeking to obtain brokerage services or investment advisory services, whether or not you provide brokerage services to the individual or establish a continuing relationship with the individual.

(ii) An individual is not your consumer if he or she provides you only with his or her name, address, and general areas of investment interest in connection with a request for a prospectus, an investment adviser brochure, or other information about financial products or services.

(iii) An individual is not your consumer if he or she has an account with another broker or dealer (the introducing broker-dealer) that carries securities for the individual in a special omnibus account with you (the clearing broker-dealer) in the name of the introducing broker-dealer, and when you receive only the account numbers and transaction information of the introducing broker-dealer's consumers in order to clear transactions.

(iv) If you are an investment company, an individual is not your consumer when the individual purchases an interest in shares you have issued only through a broker or dealer or investment adviser who is the record owner of those shares.

(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.

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

(i) *Control* of a company means the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. Any person who owns beneficially, either directly or through one or more controlled companies, more than 25 percent of the voting securities of any company is presumed to control the company. Any person who does not own more than 25 percent of the voting securities of any company will be presumed not to control the company. Any presumption regarding control may be rebutted by evidence, but, in the case of an investment company, will continue until the Commission makes a decision to the contrary according to the procedures described in section 2(a)(9) of the Investment Company Act of 1940 (15 U.S.C. 80a–2(a)(9)).

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

(k)(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:

(A) The consumer has a brokerage account with you, or if a consumer's account is transferred to you from another broker-dealer;

(B) The consumer has an investment advisory contract with you (whether written or oral);

(C) The consumer is the record owner of securities you have issued if you are an investment company;

(D) The consumer 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) The consumer purchases a variable annuity from you;

(F) The consumer has an account with an introducing broker or dealer that clears transactions with and for its customers through you on a fully disclosed basis;

(G) You hold securities or other assets as collateral for a loan made to the consumer, even if you did not make the loan or do not effect any transactions on behalf of the consumer; or

(H) You regularly effect or engage in securities transactions with or for a consumer even if you do not hold any assets of the consumer.

(ii) *No continuing relationship.* A consumer does not, however, have a continuing relationship with you if you open an account for the consumer solely for the purpose of liquidating or purchasing securities as an accommodation, *i.e.*, on a one time basis, without the expectation of engaging in other transactions.

(l) *Dealer* has the same meaning as in section 3(a)(5) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(5)).

(m) *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.

(n)(1) *Financial institution* means 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 of 1956 (12 U.S.C. 1843(k)).

(2) *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.

(o)(1) *Financial product or service* means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such 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.

(p) *G–L–B Act* means the Gramm-Leach-Bliley Act (Pub. L. No. 106–102, 113 Stat. 1338 (1999)).

(q) *Investment adviser* has the same meaning as in section 202(a)(11) of the Investment Advisers Act of 1940 (15 U.S.C. 80b–2(a)(11)).

(r) *Investment company* has the same meaning as in section 3 of the Investment Company Act of 1940 (15 U.S.C. 80a–3), and includes a separate series of the investment company.

(s)(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 solely 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)).

(t)(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 information.

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

(i) Publicly available information, except as included on a list described in paragraph (t)(1)(ii) of this section or when the publicly available information is disclosed in a manner that indicates the individual is or has been your consumer; 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 information.

(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 information, 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 information, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(u)(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 a loan or servicing a loan;

(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; or

(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.

(v)(1) *Publicly available information* means any information that you reasonably 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) *Examples.* (i) *Reasonable belief.* (A) You have a reasonable belief that information about your consumer is made available to the general public if you have confirmed, or your consumer has represented to you, that the information is publicly available from a source described in paragraphs (v)(1)(i)–(iii) of this section;

(B) You have a reasonable belief that information about your consumer is made available to the general public if you have taken steps to submit the information, in accordance with your internal procedures and policies and with applicable law, to a keeper of federal, State, or local government records that is required by law to make the information publicly available.

(C) You have a reasonable belief 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.

(D) You do not have a reasonable belief that information about a consumer is publicly available solely because that information would normally be recorded with a keeper of federal, State, or local government records that is required by law to make the information publicly available, if the consumer has the ability in accordance with applicable law to keep that information nonpublic, such as where a consumer may record a deed in the name of a blind trust.

(ii) *Government records.* Publicly available information in government records includes information in government real estate records and security interest filings.

(iii) *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.

(w) *You* means:

(1) Any broker or dealer;

(2) Any investment company; and

(3) Any investment adviser registered with the Commission under the Investment Advisers Act of 1940.

Subpart A—Privacy and Opt Out Notices

§ 248.4 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 §§ 248.14 and 248.15.

(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 §§ 248.14 and 248.15; 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 do not have a customer relationship with a consumer if you buy a loan made to the consumer but do not have the servicing rights for that loan.

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

(i) Effects a securities transaction with you or opens a brokerage account with you under your procedures;

(ii) Opens a brokerage account with an introducing broker or dealer that clears transactions with and for its customers through you on a fully disclosed basis;

(iii) Enters into an advisory contract with you (whether in writing or orally); or

(iv) Purchases shares you have issued (and the consumer is the record owner of the shares), if you are an investment company.

(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 § 248.8, 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;

(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; or

(iii) A nonaffiliated broker or dealer or investment adviser establishes a customer relationship between you and a consumer without your prior knowledge.

(2) *Examples of exceptions.* (i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if the customer's account is transferred to you by a trustee selected by the Securities Investor Protection Corporation (''SIPC'') and appointed by a United States Court.

(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 you and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service.

(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 on a web site.

(f) *Delivery.* When you are required to deliver an initial privacy notice by this section, you must deliver it according to § 248.9. If you use a short-form initial notice for non-customers according to § 248.6(d), you may deliver your privacy notice according to § 248.6(d)(3).

§ 248.5 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) The individual's brokerage account is closed;

(ii) The individual's investment advisory contract is terminated;

(iii) You are an investment company and the individual is no longer the record owner of securities you have issued; or

(iv) You are an investment company and your customer has been determined to be a lost securityholder as defined in 17 CFR 240.17a–24(b).

(c) *Special rule for loans.* If you do not have a customer relationship with a consumer under the special provision for loans in § 248.4(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 § 248.9.

§ 248.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under §§ 248.4, 248.5, and 248.8 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 §§ 248.14 and 248.15;

(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 §§ 248.14 and 248.15;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 248.13 (and no other exception 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 § 248.10(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 §§ 248.14 and 248.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 248.4 and 248.5. 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 the following categories, as applicable, and a few examples to illustrate the types of third parties in each category:

(i) Financial service providers;

(ii) Non-financial companies; and

(iii) Others.

(4) *Disclosures under exception for service providers and joint marketers.* If you disclose nonpublic personal information under the exception in § 248.13 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 which 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 to affiliates or nonaffiliated third parties except as authorized under §§ 248.14 and 248.15, 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 §§ 248.4(a)(2), 248.7(b), and 248.7(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 § 248.7.

(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 the privacy notice.

(3) You must deliver your short-form initial notice according to § 248.9. 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 § 248.9.

(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.

§ 248.7 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 § 248.10(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 § 248.6(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 together with the opt out notice;

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

(D) 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 § 248.4.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice after the initial notice in accordance with § 248.4, 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. Your opt out notice must explain how you will treat an opt out direction by a joint consumer.

(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 brokerage 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; or

(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).

(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 § 248.9.

§ 248.8 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 § 248.4, 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 §§ 248.13, 248.14, and 248.15, 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 § 248.9.

§ 248.9 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, post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service; or

(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; or

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

(i) 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

(ii) 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.

(2) *Example of reasonable expectation of receipt of annual privacy notice.* You

may reasonably expect that consumers who share an address will receive actual notice of your annual privacy notice if you deliver the notice with or in a stockholder or shareholder report under the conditions in 17 CFR 270.30d–1(f) or 17 CFR 270.30d–2(b), or with or in a prospectus under the conditions in 17 CFR 230.154.

(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 § 248.4(a)(1), the annual notice required by § 248.5(a), and the revised notice required by § 248.8, 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 paragraph (a) of this section by providing one notice to those consumers jointly.

Subpart B—Limits on Disclosures

§ 248.10 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 § 248.4;

(ii) You have provided to the consumer an opt out notice as required in § 248.7;

(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 §§ 248.13, 248.14, and 248.15.

(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 after 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 provision of brokerage services to a consumer as an accommodation, 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.

§ 248.11 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 § 248.14 or 248.15, 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 §§ 248.14 or 248.15 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 §§ 248.14(a), you may disclose that information under any exception in § 248.14 or 248.15 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 or in the ordinary course of business to your attorneys, accountants, and auditors. 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 §§ 248.14 or 248.15, 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 §§ 248.14 and 248.15:

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

(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 §§ 248.14 or 248.15, such as in the ordinary course of business to your attorneys, accountants, or auditors.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal information to a nonaffiliated third party under an exception in §§ 248.14 or 248.15, 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 §§ 248.14 or 248.15 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 §§ 248.14 or 248.15, 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.

§ 248.12 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) *Example—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.

Subpart C—Exceptions

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

(a) *General rule.* (1) The opt out requirements in §§ 248.7 and 248.10 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 § 248.4; 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 §§ 248.14 or 248.15 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 §§ 248.14 or 248.15 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.

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

(a) *Exceptions for processing and servicing transactions at consumer's request.* The requirements for initial notice in § 248.4(a)(2), for the opt out in §§ 248.7 and 248.10, and for initial notice in § 248.13 in connection with service providers and joint marketing, 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) Processing or servicing 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; or

(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.

§ 248.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to notice and opt out requirements.* The requirements for initial notice in § 248.4(a)(2), for the opt out in §§ 248.7 and 248.10, and for initial notice in § 248.13 in connection with service providers and joint marketing 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 mortgage lender of the value of the assets in the consumer's brokerage or investment advisory account so that the lender can evaluate the consumer's application for a mortgage loan.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 248.7(f).

Subpart D—Relation to Other Laws; Effective Date

§ 248.16 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.

§ 248.17 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 Federal Trade Commission, after consultation with the Commission, on the Federal Trade Commission's own motion, or upon the petition of any interested party.

§ 248.18 Effective date; transition rule.

(a) *Effective date.* 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 compliance date for this part is July 1, 2001.

(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 § 248.4, 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 § 248.13(a)(2), 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 agreement on or before July 1, 2000.

§§ 248.19–248.29 [Reserved]

§ 248.30 Procedures to safeguard customer records and information.

Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt policies and procedures that address administrative, technical, and

physical safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to:

(a) Insure the security and confidentiality of customer records and information;

(b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

(c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Appendix A to Part 248—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, 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 § 248.6(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 § 248.6(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 §§ 248.13, 248.14, and 248.15.

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 §§ 248.6(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 §§ 248.14 and 248.15.

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 § 248.6(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 §§ 248.13, 248.14, and 248.15, as well as when permitted by the exceptions in §§ 248.14 and 248.15.

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 § 248.6(a)(5) related to the exception for service providers and joint marketers in § 248.13. 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 which 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 § 248.6(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 §§ 248.13, 248.14, and 248.15.

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 § 248.6(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 standards to guard your nonpublic personal information.

By the Commission.

Dated: June 22, 2000.

Margaret H. McFarland,

Deputy Secretary.

[FR Doc. 00–16269 Filed 6–28–00; 8:45 am]

BILLING CODE 8010–01–P