SECURITIES AND EXCHANGE COMMISSION

17 CFR part 248

[Release Nos. 34–42484, IC–24326, IA–1856; File No. S7–6–00]

RIN 3235–AH90

Privacy of Consumer Financial Information (Regulation S–P)

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission requests comment on proposed Regulation S–P, privacy rules published 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 the ability of certain financial institutions to disclose nonpublic personal information about consumers to nonaffiliated third parties. 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 Gramm-Leach-Bliley Act also requires the Commission to establish for financial institutions appropriate standards to protect customer information. The proposed rules implement these requirements of the Gramm-Leach-Bliley Act with respect to financial institutions subject to the Commission's jurisdiction under that Act.

DATES: Comments must be received by March 31, 2000.

ADDRESSES: Comments should be submitted in triplicate to Jonathan G. Katz, Secretary, Securities and Exchange Commission, 450 5th Street, NW, Washington, DC 20549–0609. Comments also may be submitted electronically to the following E-mail address: rule-comments@sec.gov. All comment letters should refer to File No. S7–6–00; this file number should be included on the subject line if E-mail is used. Comment letters will be available for public inspection and copying in the Commission's Public Reference Room, 450 5th Street, NW, Washington, DC 20549. Electronically submitted comment letters will be posted on the Commission's Internet web site (http://www.sec.gov).

FOR FURTHER INFORMATION CONTACT: For information regarding the proposed rules as they relate to brokers or dealers, contact George Lavdas, Office of Chief Counsel, at the Division of Market Regulation, (202) 942–0073, or regarding the proposed rules as they relate to investment companies or investment advisers, Penelope W. Saltzman, Office of Regulatory Policy, (202) 942–0690, at the 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 proposing for public comment new Regulation S–P, 17 CFR 248.1–248.30, under the Gramm-Leach-Bliley Act [Pub. L. No. 106–102, 113 Stat. 1338 (1999), to be codified at 15 U.S.C. 6801–6809], the Securities Exchange Act of 1934 [15 U.S.C. 78a] (''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

On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act (''G–L–B Act'') [1] into law. Subtitle A of Title V of 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 such regulations as may be necessary to carry out the purposes of the provisions in Title V that govern disclosure of nonpublic personal information.

Commission representatives participated with representatives from the Agencies in drafting proposed rules to implement Title V. As is required by the G–L–B Act, the rules we are proposing today are, to the extent possible, consistent with and comparable to the rules proposed by the Agencies. Proposed Regulation S–P contains rules of general applicability that are substantially similar to the rules proposed by the banking agencies.[2] The proposed rules also contain examples that illustrate the application of the general rules. These examples differ from those used by the banking 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. The rules we are proposing today include requirements for brokers, dealers, and investment companies, as well as investment advisers registered with the Commission (''registered investment advisers''), to adopt appropriate policies and procedures that address safeguards to protect this information.

We request comment on all aspects of the proposed rules as well as comment on the specific provisions and issues highlighted in the section-by-section analysis below. We specifically request comment on the proposed examples and on any additional examples that would be helpful.

II. Section-by-Section Analysis

Section 248.1 Purpose and Scope

Proposed paragraph (a) of section 248.1 identifies three purposes of the

[1] Pub. L. 106–102, 113 Stat. 1338 (1999) (to be codified at 15 U.S.C. 6801–6809).

[2] 2. *See* G–L–B Act § 504(a). The banking agencies published a joint release proposing rules to implement Title V earlier this month. Privacy of Consumer Financial Information, 65 FR 8770 (Feb. 22, 2000) (''Banking Agencies'' Proposal''). The Federal Trade Commision proposed its privacy rules on February 24, 2000 [Privacy of Consumer Financial Information, available at <www.ftc.gov>]. The National Credit Union Administration approved its rule proposal the same day [Privacy of Consumer Financial Information, Requirements for Insurance, available at <www.ncua.gov>].

rules. First, the rules require a financial institution to provide notice to consumers about the institution's privacy policies and practices. Second, the rules describe the conditions under which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party. Third, the rules provide a method for a consumer to ''opt out'' of the disclosure of that information to nonaffiliated third parties, subject to certain exceptions discussed below.

Proposed paragraph (b) sets out the scope of the Commission's rules and lists the entities subject to the Commission's enforcement jurisdiction under section 505(a) of the G–L–B Act.[3] This paragraph notes that the rules apply only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes.

We note that other federal, State, or applicable foreign laws may impose limitations on disclosures of nonpublic personal information in addition to those imposed by the G–L–B Act and these proposed rules.[4] Thus, financial institutions will need to monitor and comply with relevant legislative and regulatory developments that affect the disclosure of consumer information.

Section 248.2 Rule of Construction

Proposed section 248.2 sets out a rule of construction intended to clarify the effect of the examples used in the rules. Given the wide variety of transactions that Title V covers, the proposal would include rules of general applicability and provide examples that are intended to assist financial institutions in complying with the rule. These examples are not intended to be exhaustive; rather, they are intended to provide guidance about how the rules are likely to apply in specific situations.[5] We invite comment on whether including examples in the rule is useful, and suggestions on additional or different examples that may be helpful in providing guidance as to the applicability of the rule.

Section 248.3 Definitions

(a) *Affiliate.* The proposed rules incorporate the definition of ''affiliate'' used in section 509(6) of the G–L–B Act. A broker, dealer, investment company, or registered investment adviser will be considered affiliated with another company if it ''controls,'' is controlled by, or is under common control with the other company.[6] The definition includes both financial institutions and entities that are not financial institutions.

The Commission's definition of control differs from the definition adopted by the Agencies.[7] The proposed rules also provide that a broker, dealer, investment company, or registered investment adviser will be considered an affiliate of another company for purposes of the privacy rules if: (i) the other company is regulated under Title V by one of the Agencies and (ii) the privacy rules adopted by that Agency treat the broker, dealer, investment company, or registered investment adviser as an affiliate of the other company.[8]

(b) *Broker.* For purposes of this part, the term ''broker'' is defined to have the same meaning as in section 3(a)(4) of the Exchange Act,[9] whether or not the institution is registered under section 15(b) of the Exchange Act.[10] The term includes a municipal securities broker as defined in section 3(a)(31) of the Exchange Act,[11] whether or not it is registered under section 15(b) of the Exchange Act.[12] The definition also includes a government securities broker as defined in section 3(a)(43) of the Exchange Act [13] (other than a bank as defined in section 3(a)(6) of the Exchange Act [14]) whether or not the broker is registered under sections 15(b) or 15C(a)(2) of the Exchange Act.[15]

(c) *Clear and conspicuous.* Title V and the proposed rules require that various notices be ''clear and conspicuous.'' The proposed rules define this term to mean that the notice is reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice.

The proposed rules do not mandate the use of any particular technique for making the notices clear and conspicuous, but instead allow each financial institution the flexibility to decide for itself how best to comply with this requirement. A notice could satisfy the clear and conspicuous standard, for instance, by using a plain-language caption, in a type set easily read, that is designed to call attention to the information contained in the notice. Other plain language principles are provided in the examples that follow the general rule.

(d) *Collect.* The proposed rules define ''collect'' to mean obtaining any

[3] Section 505(a) of the G–L–B Act requires the Commission to enforce the G–L–B Act and regulations adopted under the Act as follows: with respect to brokers and dealers under the Exchange Act, with respect to investment companies under the Investment Company Act, and with respect to investment advisers registered with the Commission under the Investment Advisers Act. Therefore, in addition to its authority under section 504 of the G–L–B Act, the Commission is proposing this part under its rulemaking authority under the Exchange Act, the Investment Company Act, and the Investment Advisers Act. Financial institutions subject to this part would also be subject to the Commission's enforcement of this part under those statutes.

[4] For example, an investment adviser may be subject to fiduciary principles under state law that impose additional limits on the adviser's ability to disclose information about its customers to any third party. *See* Restatement (Second) of Agency § 395 (an agent is subject to a duty to the principal not to use or to communicate information confidentially given him by the principal or acquired by him during the course of his agency); *General Acquisition, Inc.* v. *Gencorp Inc.,* 766 F.Supp. 1460, 1475 (S.D. Ohio 1990) (''[I]t is well settled that a fiduciary is under a duty not to disclose or use for his own benefit confidential information acquired in the course of its fiduciary relationship'').

[5] The banking agencies' proposal provides that, to the extent applicable, compliance with the examples would constitute compliance with the applicable rule. *See, e.g.,* Banking Agencies' Proposal, proposed §§ 40.2, 216.2, 332.2, 573.2. The examples in our proposed rules, however, would not provide the same safe harbor. The examples are intended to describe ordinary situations that would comply with the applicable rule, but the particular facts and circumstances relating to each specific situation will determine whether compliance with an example constitutes compliance with the rule.

[6] We have defined ''control'' for purposes of brokers, dealers, investment companies, and registered investment advisers to mean 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. *See infra* discussion of proposed section 248.3(i).

[7] Under the Banking Agencies' Proposal, for example, control means ownership of 25 percent of a company's voting securities, control over the election of a majority of the directors, trustees or general partners of the company, or the power to exercise a controlling influence over management or policies of a company, as determined by the particular agency. *See, e.g.,* Banking Agencies' Proposal, proposed §§ 40.3(g), 216.3(g), 332.3(g), 573.3(g).

[8] Proposed § 248.3(a)(1)–(2). This part of the proposed definition is designed to prevent the disparate treatment of affiliates within a holding company structure. Without this provision, a broker-dealer in a bank holding company structure might not be considered affiliated with another entity in that organization under the Commission's proposed rules, even though the two entities would be considered affiliated under the Banking Agencies' Proposal.

[9] 15 U.S.C. 78c(a)(4).

[10] 15 U.S.C. 78o(b).

[11] 15 U.S.C. 78c(a)(31).

[12] 15 U.S.C. 78o(b).

[13] 15 U.S.C. 78c(a)(43).

[14] 15 U.S.C. 78c(a)(6). For purposes of this definition and the definition of ''dealer'' (*see* proposed § 248.3(l)), the term ''bank'' does not include a foreign bank (as that term is defined in section 1(b)(7) the International Banking Act of 1978, 12 U.S.C. 3101(7)) or a savings association (as defined in section 3(b) of the Federal Deposit Insurance Act, 12 U.S.C. 1813(b)) the deposits of which are insured by the Federal Deposit Insurance Corporation.

[15] 15 U.S.C. 78o(b), 78o–5(a)(2).

information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information. Several sections of the proposed rules impose obligations that arise when a financial institution collects information about a consumer.[16] This proposed definition clarifies that these obligations arise when the information enables the user to identify a particular consumer. It also clarifies that the obligations arise regardless of whether the financial institution obtains the information from a consumer or from some other source.

(f) *Company.* The proposed rules define ''company,'' which is used in the definition of ''affiliate,'' as any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

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

The G–L–B Act distinguishes ''consumers'' from ''customers'' for purposes of the notice requirements imposed by the Act. As explained below in the discussion of proposed section 248.4, a financial institution must 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 a purpose that is not authorized by one of several exceptions set out in proposed sections 248.10 and 248.11. By contrast, a financial institution must give all ''customers,'' at the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship, a notice of the institution's privacy policy.

A person is a ''consumer'' under the proposed rules if he or she obtains a financial product or service from a financial institution. The definition of ''financial product or service'' in proposed section 248.3(n) includes, among other things, a financial institution's evaluation of an individual's application to obtain a financial product or service. Thus, a financial institution that intends to share nonpublic personal information about a consumer with nonaffiliated third parties outside of the exceptions described in sections 248.10 and 248.11 will have to give the requisite notices, even if the consumer does not enter into a customer relationship with the institution.

The examples that follow the definition of ''consumer'' explain when someone is a consumer. The examples clarify that a consumer includes someone who provides nonpublic personal information in connection with seeking to obtain brokerage or investment advisory services, but does not include someone who provides only name, address, and areas of investment interest in order to obtain a prospectus, investment adviser brochure, or other information about a financial product.[17] An individual who has an account with an introducing broker and whose securities are carried by a clearing broker in a special omnibus account in the name of the introducing broker is not a consumer for purposes of the clearing broker if it receives no nonpublic personal information about the consumer. Similarly, investment company shareholders who are not the record owners of their shares would not be consumers for purposes of the investment company.[18]

(h) *Consumer reporting agency.* The proposed rules incorporate the definition of ''consumer reporting agency'' in section 603(f) of the Fair Credit Reporting Act.[19] This term is used in proposed sections 248.11 and 248.13.

(i) *Control.* The proposed rules define ''control'' for purposes of brokers, dealers, investment companies, and registered investment advisers to mean the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise.[20] In addition, ownership of more than 25 percent of a company's voting securities creates a presumption of control of the company.[21] This definition is used to determine when companies are affiliated,[22] and would result in financial institutions being considered as affiliates regardless of whether the control is exercised by a company or individual.

(j) *Customer.* The proposed rules define ''customer'' as any consumer who has a ''customer relationship'' with a particular financial institution. As explained more fully in the discussion of proposed section 248.4 below, a consumer becomes a customer of a financial institution when he or she enters into a continuing relationship with the institution. For example, a consumer would become a customer when he or she enters into an investment advisory contract (whether written or oral), completes the documents needed to open a brokerage account, or purchases shares of an investment company in his or her own name.

The distinction between consumers and customers determines the notices that a financial institution must provide. If a consumer never becomes a customer, the institution is not required to provide any notices to the consumer unless the institution intends to disclose nonpublic personal information about that consumer to nonaffiliated third parties (outside of the exceptions as set out in sections 248.10 and 248.11). By contrast, if a consumer becomes a customer, the institution must provide a copy of its privacy policy before it establishes the customer relationship and at least annually during the continuation of the customer relationship.

(k) *Customer relationship.* The proposed rules define ''customer relationship'' as a continuing relationship between a consumer and a financial institution in which the institution provides a financial product or service that is to be used by the consumer primarily for personal, family, or household purposes. Because the G–L–B Act requires annual notices of the financial institution's privacy policies to its customers, we have interpreted the Act as requiring more than isolated transactions between a financial institution and a consumer to establish a customer relationship, unless it is reasonable to expect further contact about that transaction between the institution and consumer afterwards. Thus, the proposed rules define ''customer relationship'' as one that generally is of a continuing nature. As noted in the examples that follow the definition, this would include a brokerage account or investment advisory relationship. A broker would have a customer relationship with a consumer when the broker regularly effects securities transactions for the

[16] *See, e.g.,* proposed §§ 248.6, 248.7.

[17] Individuals may provide this information, for example, on ''tear-out'' cards from magazines, or in telephone or Internet requests for prospectuses or brochures.

[18] *See also infra* discussion of proposed section 248.3(k) (definition of ''customer relationship'').

[19] 15 U.S.C. 1681a(f).

[20] *See, e.g.*, 17 CFR 240.19g2–1(b)(2).

[21] This presumption 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 [15 U.S.C. 80a–2(a)(9)].

[22] *See* discussion of proposed § 248.3(a), *supra.*

customer, even if the broker holds none of the customer's assets.

A one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. The examples that follow the definition of ''customer relationship'' clarify that an individual's purchase of securities through a broker with whom the customer opens an account would be sufficient to establish a customer relationship because of the continuing nature of the service. The individual would be a customer even if the account is established only to hold securities or other assets as collateral for a loan made by another institution. By contrast, an individual who purchases securities through a broker would not be the broker's customer if the broker provides the service as an accommodation but does not open an account for the individual.[23] Similarly, a consumer does not become a broker's customer when the broker liquidates securities for the consumer on a one-time basis.

The examples also clarify that a consumer will have a customer relationship with an investment company whose shares the consumer owns in his or her own name, even if the consumer purchased those shares through a broker or investment adviser. In that case, the individual will be a customer of both the broker or investment adviser who sold the shares *and* the investment company. Similarly, an introducing broker's customer will also be a customer of the broker that clears customer transactions for the introducing broker on a fully disclosed basis.

(l) *Dealer.* The proposed rules define the term ''dealer'' to have the same meaning as in section 3(a)(5) of the Exchange Act,[24] whether or not the dealer is registered under section 15(b) of the Exchange Act. The term includes a municipal securities dealer as defined in section 3(a)(30) of the Exchange Act,[25] other than a bank (as defined in section 3(a)(6) of the Exchange Act [26]), whether or not the dealer is registered under sections 15(b) or 15B(a)(2) of the Exchange Act. The term also includes a government securities dealer as defined in section 3(a)(44) of the Exchange Act,[27] whether or not the dealer is registered under sections 15(b) or 15C(a)(2) of the Exchange Act.

(m) *Financial institution.* The proposed rules define ''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 (''Bank Holding Company Act''),[28] including brokers, dealers, investment companies, and registered investment advisers. The proposed rules also exempt from the definition of ''financial institution'' those entities specifically excluded by the G–L–B Act.

(n) *Financial product or service.* The proposed rules define ''financial product or service,'' for purposes of Regulation S–P only, as a product or service that a financial institution could offer as 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), is not included in the definition of ''financial product or service'' under this part. The proposed definition includes the financial institution's evaluation of information collected in connection with an application by a consumer for a financial product or service even if the application ultimately is rejected or withdrawn. It also includes the distribution of information about a consumer for the purpose of assisting the consumer to obtain a financial product or service. To avoid confusion as to whether an investment company shareholder is an owner or a customer of the institution, the proposed definition clarifies that, for purposes of this regulation, the term ''financial product'' includes shares of an investment company.

(p) *Government regulator.* The proposed rules define ''government regulator'' to include the Commission and each of the Agencies and State insurance authorities. This term is used in two places. First, the term is used in proposed section 248.3(a), the definition of ''affiliate.'' Second, the term is used in the exception set out in proposed section 248.11(a)(4) for disclosures to law enforcement agencies, ''including government regulators.''

(q) *Investment adviser.* The proposed definition incorporates the definition of investment adviser in section 202(a)(11) of the Investment Advisers Act.[29]

(r) *Investment company.* The proposed definition incorporates the meaning of investment company in section 3 of the Investment Company Act, whether or not the investment company is registered with the Commission.[30] The definition also clarifies that the term includes a separate series of an investment company.

(s) *Nonaffiliated third party.* Paragraph (1) of the proposed definition of ''nonaffiliated third party'' provides that the term means any person (which is defined in proposed section 248.3(u) and includes natural persons as well as legal entities such as corporations, partnerships, and trusts) except (i) an affiliate of a financial institution, and (ii) a joint employee of a financial institution and a third party. This paragraph is intended to be substantively the same as the definition used in section 509(5) of the G–L–B Act.

(t) *Nonpublic personal information.* Section 509(4) of the G–L–B Act defines ''nonpublic personal information'' to mean ''personally identifiable financial information'' (which the Act does not define) that (i) is provided by a consumer to a financial institution, (ii) results from any transaction with the consumer or any service performed for the consumer, or (iii) is otherwise obtained by the financial institution. ''Nonpublic personal information'' 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.

The proposed rules implement this provision of the G–L–B Act by restating, in paragraph (1) of proposed section 248.3(t), the general categories of information described above. Paragraph (2) provides that ''nonpublic personal information'' does not include publicly available information when the information is part of a list, description, or other grouping of consumers that is derived without using personally identifiable financial information.[31] The definition also excludes any other publicly available information, unless the information is part of a list, description, or other grouping of consumers that is derived using

[23] The individual would, however, be a consumer for purposes of the broker, which would require the broker to provide notices *if* it intends to disclose nonpublic personal information about the consumer to nonaffiliated third parties outside of the exceptions.

[24] 15 U.S.C. 78c(a)(5).

[25] 15 U.S.C. 78c(a)(30).

[26] *See supra* note 14.

[27] 15 U.S.C. 78c(a)(44).

[28] 12 U.S.C. 1843(k).

[29] 15 U.S.C. 80b–2(a)(11).

[30] 15 U.S.C. 80a–3. Thus, a business development company, which is an investment company but is not required to register with the Commission, would be subject to this part. *See* 15 U.S.C. 80a–2(a)(48).

[31] Nonpublic personal information does include publicly available information that is disclosed in a manner that otherwise indicates the individual is a financial institution's consumer. *See* proposed § 248.3(t)(2)(i). We believe that, in most cases, sharing information (including publicly available information) about a consumer with a third party identifies the individual as the institution's consumer.

personally identifiable financial information.

We invite comment on whether the definition of ''nonpublic personal information'' should cover information about a consumer that contains no indicators of a consumer's identity. For example, if a broker provided aggregate information about its brokerage accounts (such as securities transaction information) to a nonaffiliated third party for the purpose of preparing market studies, should the broker, without giving notice or opportunity to opt out to the consumer, be permitted to do so if the information contains no personal identifiers?

(v) *Personally identifiable financial information.* As discussed above, the G–L–B Act defines ''nonpublic personal information'' to include, among other things, ''personally identifiable financial information'' but does not define the latter term. As a general matter, the proposed rules treat any personally identifiable information as financial if the financial institution obtains the information in connection with providing a financial product or service to a consumer. We believe that this approach reasonably interprets the word ''financial'' and creates a workable and clear standard for distinguishing information that is financial from other personal information. This interpretation would cover a broad range of personal information provided to a financial institution, including, for example, information about the consumer's health.

The proposed rules define ''personally identifiable financial information'' to include three categories of information. The first category includes any information that a consumer provides a financial institution in order to obtain a financial product or service from the institution. As noted in the examples that follow the definition, this would include information provided when opening a brokerage account, entering into an investment advisory contract, or obtaining a margin loan or a financial plan. If, for example, a consumer provides medical information on an application to obtain a financial product or service (such as a variable life insurance contract offered by an insurance company separate account), that information would be considered ''personally identifiable financial information'' for purposes of the proposed rules. Similarly, information that may be required for financial planning purposes, including details about retirement and family obligations, such as the care of a disabled child, would be covered by the definition.

The second category includes any information about a consumer resulting from any transaction between the consumer and the financial institution involving a financial product or service. This would include, as noted in the examples following the definition, information about account balance, payment or overdraft history, credit or debit card purchases, securities positions, or financial products purchased or sold.

The third category includes any financial information about a consumer otherwise obtained by the financial institution in connection with providing a financial product or service.

This would include, for example, information obtained from a consumer report or from an outside source to verify information a consumer provides on an application to obtain a financial product or service. It would not, however, include information that is publicly available (unless, as previously noted, the information is part of a list of consumers that is derived using personally identifiable financial information).

The examples clarify that the definition of ''personally identifiable financial information'' does not include a list of names and addresses of people who are customers of an entity that is not a financial institution. Thus, the names and addresses of people who subscribe, for instance, to a particular magazine would fall outside the definition. The Commission seeks comment on whether further definition of ''personally identifiable financial information'' would be helpful.

(w) *Publicly available information.* The proposed rules define ''publicly available information'' as information the financial institution reasonably believes is lawfully made available to members of the general public from three broad types of sources.[32] First, it includes information from official public records, such as real estate recordations or security interest filings. Second, it includes information from widely distributed media, such as a telephone book, radio program, or newspaper. Third, it includes information from disclosures required to be made to the general public by federal, State, or local law, such as securities disclosure documents. The proposed rules state that information obtained over the Internet will be considered publicly available information if the information is obtainable from a site available to the general public without requiring a password or similar restriction. The Commission invites comment on what information is appropriately considered publicly available, particularly in the context of information available over the Internet.

The proposed rules treat information as publicly available if it **COULD** be obtained from one of the public sources listed in the rules. If an institution reasonably believes the information is lawfully made available to the general public from one of the listed public sources, then the information will be considered publicly available and excluded from the scope of ''nonpublic personal information,'' whether or not the institution obtains it from a publicly available source (unless, as previously noted, it is part of a list of consumers that is derived using personally identifiable financial information). Under this approach, the fact that a consumer has given information to a financial institution would not automatically extend to that information the protections afforded to nonpublic personal information.

The Commission invites comment on whether the proposed definition of ''publicly available information'' should treat information that is publicly available as nonpublic if the institution does not *obtain* the information from a listed public source (''alternative definition'').[33] In many cases, the proposed definition and the alternative definition would result in the same treatment of information that may be publicly available. For example, under either definition, names and addresses that are publicly available would be treated as nonpublic personal information if they appear in a customer list. An institution that intends to share a customer list containing that information with nonaffiliated third parties would have to comply with the proposed rule's notice and opt out requirements. The alternative definition could, however, result in different notice and opt out requirements when an institution shares information available from public sources about individual customers. In that situation the proposed definition would not require the institution to comply with notice and opt out requirements as long

[32] We recognize that some information that is available to the general public may have been published illegally. In some cases, such as a list of customer account numbers posted on a web site, the publication will be obviously unlawful. In other cases, the legality of the publication may be unclear or unresolved. The proposed rule would provide that information is ''publicly available'' if the institution reasonably believes that informaiton is lawfully available to the public.

[33] The Banking Agencies Proposal (other than the Federal Reserve Board, which proposed the same definition as the Commission) includes this alternative definition. *See, e.g.*, Banking Agencies' Proposal, proposed §§ 40.3(n)–(p), 573.3(n)–(p), Alternatives A and B.

as the institution did not share the information in a manner that would indicate that the individual is or had been the institution's customer. The alternative definition, however, would require compliance with the notice and opt out requirements because the institution did not obtain the information from a public source.

(q) *You.* The term ''you'' is used in order to make the rules easier to understand and use. The proposed definition refers to the entities within the Commission's jurisdiction under Title V. The term includes brokers, dealers, investment companies, and registered investment advisers.

Section 248.4 Initial Notice to Consumers of Privacy Policies and Practices Required

Initial notice required. The G–L–B Act requires a financial institution to provide an initial notice of its privacy policies and practices in two circumstances. For customers, the notice must be provided at the time of establishing a customer relationship. For consumers who do not (or have not yet) become customers, the notice must be provided before disclosing nonpublic personal information about the consumer to a nonaffiliated third party.

Paragraph (a) of proposed section 248.4 states the general rule regarding these notices. A financial institution must provide a clear and conspicuous [34] notice that accurately reflects the institution's privacy policies and practices. Thus, a financial institution must maintain the protections that the notice represents the institution will provide. The Commission expects that brokers, dealers, investment companies, and registered investment advisers will take appropriate measures to adhere to their stated privacy policies and practices.

The proposed rules do not prohibit two or more institutions from providing a joint initial, annual, or opt out notice, as long as the notice is delivered in accordance with the rule and is accurate for all recipients. For example, institutions that could give a joint initial, annual, or opt out notice include: (i) An introducing broker and its clearing broker (that clears on a fully disclosed basis) and (ii) an investment company and a broker-dealer that distributes its shares. The rules also do not preclude an institution from establishing different privacy policies and practices for different categories of consumers, customers, or products, if each particular consumer or customer receives a notice that is accurate with respect to that individual.

Notice to customers. The proposed rules require that a financial institution provide an individual a privacy notice prior to the time that it establishes a customer relationship. Thus, the notices may be provided at the same time a financial institution is required to give other notices, such as the requirement that credit terms in margin transactions be disclosed under Exchange Act rule 10b–16,[35] or that customers be notified in writing of the existence of a carrying or clearing arrangement for accounts introduced on a fully disclosed basis to another broker, under rules applicable to members of the New York Stock Exchange and National Association of Securities Dealers.[36] This approach is intended to strike a balance between (i) ensuring that consumers will receive privacy notices at a meaningful point when ''establishing a customer relationship'' and (ii) minimizing unnecessary burdens on financial institutions that may result if a financial institution is required to provide a consumer with a series of notices at different times in a transaction. Nothing in the proposed rules is intended to discourage a financial institution from providing an individual with a privacy notice at an earlier point in the relationship if the institution wishes to do so in order to help the individual compare its privacy policies with those of other institutions before conducting transactions.

Paragraph (c) of proposed section 248.4 identifies the time a customer relationship is established as the point at which a financial institution and a consumer enter into a continuing relationship. The examples in paragraph (c) clarify that, for customer relationships that are contractual in nature (including, for example, investment advisory relationships), a customer relationship is established when the consumer enters into the contract (whether in writing or orally) that is necessary to conduct the transaction in question. Thus, a customer relationship is established with a broker-dealer when a consumer executes a securities trade through the broker-dealer or opens a brokerage account with the broker-dealer under its procedures.[37] The examples further clarify that a consumer who opens an account with an introducing broker establishes a customer relationship with the introducing broker's clearing broker (that clears on a fully disclosed basis) at the same time. Similarly, when a consumer purchases investment company shares (in his or her own name) through a principal underwriter, the consumer establishes a customer relationship with the underwriter and the investment company. We request comment on whether there are different times at which customer relationships with brokers, dealers, investment companies, or investment advisers are established.

Notice to consumers. For consumers who do not establish a customer relationship, the initial notice may be provided at any point before the financial institution discloses nonpublic personal information to nonaffiliated third parties. As provided in paragraph (b) of the proposed rule, if the institution does not intend to disclose the information in question or intends to make only those disclosures that are authorized by one of the exceptions for, among other things, processing and servicing accounts or as required by law,[38] the institution is not required to provide the initial notice.

How to provide notice. Paragraph (d) of proposed section 248.4 sets out the rules governing how financial institutions must provide the initial notices. The general rule requires that the initial notice be provided so that each recipient can reasonably be expected to receive actual notice. The Commission invites comment on who should receive a notice in situations in which there is more than one party to an account.

The notice may be delivered in writing or, if the consumer agrees, electronically. Oral notices alone are insufficient. In the case of customers, the notice must be given in a way so that the customer may either retain it or access it at a later time.[39]

Examples of acceptable ways to deliver the notice include hand-delivering a copy of the notice, mailing a copy to the consumer's last known address, or sending it by electronic mail

[34] *See* proposed § 248.3(c).

[35] 17 CFR 240.10b–16.

[36] *See* Rule 382 of the New York Stock Exchange, Inc. (''NYSE'') Operation of Member Organizations, NYSE Guide (CCH) 3639–40 (1999); Rule 3230 of the National Association of Securities Dealers (''NASD'') Conduct Rules, NASD Manual (CCH) 4922 (1999).

[37] As indicated in the examples under the definition of a customer relationship, we do not believe that a customer relationship exists when a broker-dealer executes a securities trade for a consumer as an accommodation or to liquidate securities on a one-time basis, *i.e.*, when there is no expectation of further transactions.

[38] *See* proposed §§ 248.10 and 248.11.

[39] The requirement that the notice be given in a manner permitting access at a later time does not preclude a financial institution from changing its privacy policy. *See* proposed § 248.8(c). Rather the requirement is intended to provide that a customer will be able to access the most recently adopted privacy policy.

to a consumer who obtains a financial product or service from the institution electronically. It would not be sufficient to provide only a posted copy of the notice in a lobby. Similarly, it would not be sufficient to provide the initial notice only on a Web page, unless the consumer is required to access that page to obtain the product or service in question. Electronic delivery generally should be in the form of electronic mail to ensure that a consumer actually receives the notice. In those circumstances in which a consumer is in the process of conducting a transaction over the Internet, electronic delivery also may include posting the notice on a Web page as described above. If a financial institution and consumer enter into a contract for a financial product or service over the telephone, the institution may provide the consumer with the option of receiving the initial notice after providing the product or service in order not to delay the transaction. We invite comment on the regulatory burden of providing the initial notices and on the methods financial institutions anticipate using to provide the notices. We also request comment on whether there are additional circumstances in which an institution should be permitted to provide notices within a reasonable time after the customer relationship is established.

Section 248.5 Annual Notice to Customers Required

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

Section 503(a) of the G–L–B Act requires that the annual notices be provided ''during the continuation'' of a customer relationship. To implement this requirement, the proposed rules state that a financial institution is not required to provide annual notices to a customer with whom it no longer has a continuing relationship.[40] The examples that follow this general rule provide guidance on when there no longer is a continuing relationship for purposes of the rules.

These include, for instance, a brokerage account that has been closed or an investment advisory contract that has been terminated. In addition, an investment company shareholder who has redeemed all of his or her shares or is determined to be a lost securityholder under rule 17a–24 under the Exchange Act would no longer be considered to be a customer of the investment company.[41]

The Commission invites comment generally on whether the examples provided in proposed section 248.5 are adequate and whether there are other situations in which an individual may have an account with an institution but the customer relationship has ended. We also invite comment on the regulatory burden of providing the annual notices and on the methods financial institutions anticipate using to provide the notices.

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

Section 503 of the G–L–B Act identifies the items of information that must be included in a financial institution's initial and annual notices. Section 503(a) of the G–L–B Act establishes 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 the notice must address.

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

The information to be included is as follows:

1. *Categories of nonpublic personal information that a financial institution may collect.* Section 503(b)(2) requires a financial institution to inform its customers about the categories of nonpublic personal information that the institution collects. The proposed rules implement this requirement in section 248.6(a)(1) and provide an example of how to comply with this requirement that focuses the notice on the source of the information collected. As noted in the example, a financial institution will satisfy this requirement if it categorizes the information according to the sources, such as application information, transaction information, and consumer report information. Financial institutions may provide more detail about the categories of information collected but are not required to do so.

2. *Categories of nonpublic personal information that a financial institution may disclose.* Section 503(a)(1) of the G–L–B Act requires the financial institution's initial and annual notice to provide information about the categories of nonpublic personal information that may be disclosed either to affiliates or nonaffiliated third parties. The proposed rules implement this requirement in proposed section 248.6(a)(2). The examples of how to comply with this rule focus on the content of information to be disclosed. A financial institution may satisfy this requirement by categorizing information according to source and providing examples of the content of the information. These categories might include application information (such as assets, income, investment goals, and investment risk tolerance), identifying information (such as name, address, and social security number), transaction information (such as information about account activity, account balances, securities positions, and securities purchases and sales), and information from consumer reports (such as credit history).

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

3. *Categories of affiliates and nonaffiliated third parties to whom a financial institution discloses nonpublic personal information.* As previously noted, section 503(a) of the G–L–B Act includes a general requirement that a financial institution provide a notice to its customers of the institution's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) states that the notice

[40] Proposed § 248.5(c).

[41] 17 CFR 240.17a–24. This rule requires recordkeeping transfer agents to file reports with the Commission on lost securityholder accounts. A ''lost securityholder'' is a securityholder to whom correspondence has been sent at the address contained in the transfer agent's master securityholder file, that has been returned as undeliverable and for whom the transfer agent has not received information regarding a new address. 17 CFR 240.17a–24(b). The definition permits the transfer agent to deem the securityholder lost as of the date the item has been returned as undeliverable after having been re-sent.

required by section 503(a) must include certain specified items. Among those is the requirement, set out in section 503(b)(1), that a financial institution inform its customers about its policies and practices with respect to disclosing nonpublic personal information to nonaffiliated third parties. We believe that sections 503(a) and 503(b) of the G–L–B Act require a financial institution's notice to address disclosures of nonpublic personal information to both affiliates and nonaffiliated third parties.

The proposed rules implement this notice requirement in section 248.6(a)(3). The example states that a financial institution will adequately categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic personal information about consumers if it identifies the types of businesses in which they engage. Types of businesses may be described by general terms, such as financial products or services, if the financial institution provides examples of the significant lines of businesses of the recipient, such as retail banking, mortgage lending, life insurance, or securities brokerage.

The G–L–B Act does not require a financial institution to list the categories of persons to whom information may be disclosed under any of the exceptions set out in proposed sections 248.10 and 248.11. The proposed rules state that a financial institution is required only to inform consumers that it makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the notice. We invite comment on whether such a notice would be adequate.

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

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

We have concluded that sections 503(a)(2) and 503(b)(1)(B) require a financial institution to include in the initial and annual notices the institution's policies and practices with respect to sharing information about former customers with all affiliates and nonaffiliated third parties. This requirement is set out in the proposed rules at section 248.6(a)(4). This provision does not require a financial institution to provide a notice to a former customer before sharing nonpublic personal information about that former customer with an affiliate.[42]

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

The proposed rules implement these provisions, in section 248.6(a)(5), by requiring that, if a financial institution discloses nonpublic personal information to a nonaffiliated third party under the exception for service providers and joint marketing, the institution is to include in the initial and annual notices a separate description of the categories of information that are disclosed and the categories of third parties providing the services. A financial institution may comply with these requirements by providing the same level of detail in the notice as is required to satisfy proposed sections 248.6(a)(2) and (3).

6. *Right to opt out.* As previously noted, sections 503(a)(1) and 503(b)(1) of the G–L–B Act require a financial institution to provide customers with a notice of its privacy policies and practices concerning, among other things, disclosing nonpublic personal information consistent with section 502 of the Act. Proposed rule 248.6(a)(6) implements this section by requiring the initial and annual notices to explain the right to opt out of disclosures of nonpublic personal information to nonaffiliated third parties, including the methods available to exercise that right.

7. *Disclosures made under the FCRA.* Section 503(b)(4) of the G–L–B Act requires a financial institution's initial and annual notice to include the disclosures required, if any, under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (''FCRA'').[43] Section 603(d)(2)(A)(iii) excludes from the definition of ''consumer report'' (and, therefore, the protections provided under the FCRA for information contained in those reports) the communication of certain consumer information among affiliated entities if the consumer is notified about the disclosure of that information and given an opportunity to opt out of the information sharing. The information that can be shared among affiliates under this provision includes, for instance, information from consumer reports and applications for financial products or services. In general, this information represents personal information provided directly by the consumer to the institution, such as income and social security number, in addition to information contained within credit bureau reports.

The proposed rules implement section 503(b)(4) of the G–L–B Act by including the requirement that a financial institution's initial and annual notice include any disclosures a financial institution makes under section 603(d)(2)(A)(iii) of the FCRA.[44]

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

The proposed rules implement these provisions by requiring a financial institution to include in the initial and annual notices the institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.[45] The example in the proposed rules states that a financial institution may comply with the requirement as it concerns confidentiality and security if the institution explains matters such as who has access to the information and the

[42] An institution that intends to share nonpublic personal information about a former customer with a nonaffiliated third party would be required to provide the customer with notice and opportunity to opt out before sharing the information with the third party.

[43] 15 U.S.C. 1681a(d)(2)(A)(iii).

[44] *See* proposed § 248.6(a)(7).

[45] *See* proposed § 248.6(a)(8).

circumstances under which the information may be accessed. The information about integrity should focus on the measures the institution takes to protect against reasonably anticipated threats or hazards. The proposed rules do not require a financial institution to provide technical or proprietary information about how it safeguards consumer information.[46]

Section 248.7 Limitation on Disclosure of Nonpublic Personal Information About Consumers to Nonaffiliated Third Parties

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

Section 248.7 of the proposed rules implements these provisions. Paragraph (a)(1) of section 248.7 sets out the criteria that a financial institution must satisfy before disclosing nonpublic personal information to nonaffiliated third parties. As stated in the text of the proposed rules, these criteria apply to direct and indirect disclosures through an affiliate. We invite comment on how the right to opt out should apply in the case of joint accounts. Should, for instance, a financial institution require all parties to an account to opt out before the opt out becomes effective? If not and only one of the parties opts out, should the opt out apply only to information about the party opting out or should it apply to information about all parties to the account? We also request comment on how the opt out right should apply to an investment adviser who manages a trust account on behalf of multiple beneficiaries.

Paragraph (a)(2) defines ''opt out'' in a way that incorporates the exceptions to the right to opt out stated in proposed sections 248.9, 248.10, and 248.11, which permit disclosures of nonpublic personal information to nonaffiliated third parties without first providing the initial privacy notice and giving the consumer the right to opt out.

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

The requirement that a consumer have a reasonable opportunity to opt out does not mean that a consumer forfeits that right once the opportunity lapses. The consumer always has the right to opt out (as discussed further in proposed section 248.8, below). However, if an individual does not exercise that opt out right when first presented with an opportunity, the financial institution would be permitted to disclose nonpublic personal information to nonaffiliated third parties during the period of time before it implements the consumer's opt out direction.

Paragraph (b) of proposed section 248.7 clarifies that the right to opt out applies regardless of whether a consumer has established a customer relationship with a financial institution. As noted above, all customers are consumers under the proposed rules. Thus, the fact that a consumer establishes a customer relationship with a financial institution does not change the institution's obligations to comply with the requirements of proposed section 248.7(a) before sharing nonpublic personal information about that consumer with nonaffiliated third parties. This also applies in the context of a consumer who had a customer relationship with a financial institution but then terminated that relationship. Paragraph (b) also clarifies that the consumer protections afforded by paragraph (a) of proposed section 248.7 apply to all nonpublic personal information collected by a financial institution, regardless of when collected. Thus, if a consumer elects to opt out of information sharing with nonaffiliated third parties, that election applies to all nonpublic personal information about that consumer in the financial institution's possession, regardless of when the information is obtained.

Paragraph (c) of proposed section 248.7 states that a financial institution may, but is not required to, provide consumers with the option of a partial opt out in addition to the opt out required by this section. This could enable a consumer to limit, for instance, the types of information disclosed to nonaffiliated third parties or the types of recipients of the nonpublic personal information about that consumer. If the partial opt out option is provided, a financial institution must state this option in a way that clearly informs the consumer about the choices available and the resulting consequences.

Section 248.8 Form and Method of Providing Opt Out Notice to Consumers

Paragraph (a) of proposed section 248.8 requires that any opt out notice provided by a financial institution pursuant to proposed section 248.7 be clear and conspicuous, and accurately explain the right to opt out. The notice must inform the consumer that the institution may disclose nonpublic personal information to nonaffiliated third parties, state that the consumer has a right to opt out, and provide the consumer with a reasonable means by which to opt out.

The examples that follow the general rule state that a financial institution will adequately provide notice of the right to opt out if it identifies the categories of information that may be disclosed and the categories of nonaffiliated third parties to whom the information may be disclosed and explains that the consumer may opt out of those disclosures. A financial institution that plans to disclose only limited types of information or to only a specific type of nonaffiliated third party may provide a correspondingly narrow notice to consumers. However, to minimize the number of opt out notices a financial institution must provide, the institution may wish to base its notices on current and anticipated information sharing plans. A new opt out notice is not required for disclosures to different types of nonaffiliated third parties or of different types of information, provided that the most recent opt out notice is sufficiently broad to cover the entities or information in question. A financial institution also need not provide subsequent opt out notices when a consumer establishes a new type of customer relationship with that financial institution, unless the

[46] The proposed rules require brokers, dealers, investment companies, and registered investment advisers to adopt policies and procedures relating to administrative, technical, and physical safeguards (*see* proposed § 248.30).

institution's opt out policies differ based on the type of customer relationship.

The examples suggest several ways in which a financial institution may provide reasonable means to opt out, including check-off boxes, reply forms, and electronic mail addresses. A financial institution does not provide a reasonable means to opt out if the only means provided is for consumers to send their own letters to the institution to exercise their right, although an institution may honor such a letter if received. We also invite comment on whether a financial institution that provides its notice electronically also should be required to provide an electronic means to opt out.

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

Paragraph (c) sets out the rules governing a financial institution's obligations in the event the institution changes its disclosure policies. As stated in that paragraph, a financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless the institution first provides a revised notice and new opportunity to opt out. The institution must wait a reasonable period of time before disclosing information according to the terms of the revised notice in order to afford the consumer a reasonable opportunity to opt out. A financial institution must provide a consumer the revised notice of its policies and practices and opt out notice by using the means permitted for providing the initial notice and opt out notice to that consumer under section 248.4(d) and section 248.8(b), respectively, which require that the notices be given in a manner so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form.

Paragraph (d) states that a consumer has the right to opt out at any time. We considered whether to include a time limit by which financial institutions must effectuate a consumer's opt out, but decided that the wide variety of practices of financial institutions made one limit inappropriate. Instead, the proposed rules require a financial institution to stop sharing information as soon as reasonably practicable. We request comment on whether the rules should specify a time within which an institution must stop sharing information, and if so, what the time period should be.

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

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

Section 248.9 Exception To Opt Out Requirements for Service Providers and Joint Marketing

Section 502(b)(2) of the G–L–B Act creates an exception to the opt out rules for the disclosure of information to a nonaffiliated third party for its use 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 under a joint agreement between two or more financial institutions. A consumer will not have the right to opt out of disclosing nonpublic personal information about the consumer to nonaffiliated third parties under these circumstances, if the financial institution satisfies certain requirements.

First, the institution must, as stated in section 502(b)(2), ''fully disclose'' to the consumer that it will provide this information to the nonaffiliated third party before the information is shared. This disclosure could appear in the initial notice required by section 248.4. We invite comment on whether the proposed rules appropriately implement the ''fully disclose'' requirement in section 502(b)(2).

Second, the financial institution must enter into a contract with the third party that requires the third party to maintain the confidentiality of the information. This contract should be designed to ensure that the third party (a) will maintain the confidentiality of the information at least to the same extent as is required for the financial institution that discloses it, and (b) will use the information solely for the purposes for which the information is disclosed or as otherwise permitted by sections 248.10 and 248.11 of the proposed rules.

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

Section 248.10 Exceptions for Processing and Servicing Transactions

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

Paragraph (a) of proposed section 248.10 sets out those exceptions, making only stylistic changes to the statutory text that are intended to make the exceptions easier to read. Paragraph (b) sets out the definition of ''necessary to effect, administer, or enforce'' that is contained in section 509(7) of the G–L–B Act, making only stylistic changes intended to clarify the definition.

The exceptions set out in proposed section 248.10, and the exceptions discussed in proposed section 248.11, below, do not affect a financial institution's obligation to provide initial notices of its privacy policies and practices prior to the time it establishes a customer relationship and annual notices thereafter. Those notices must be provided to all customers, even if the institution intends to disclose the nonpublic personal information only under the exceptions in proposed section 248.10.

Section 248.11 Other Exceptions To 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. Proposed section 248.11 sets out those exceptions that are not made in connection with

the administration, processing, servicing, or sale of a consumer's account, and makes stylistic changes intended to clarify the exceptions.

One of the exceptions stated in proposed section 248.11 is for disclosures made with the consent or at the direction of the consumer, provided the consumer has not revoked the consent. Following the list of exceptions is an example of consent in which a consumer 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. Consent in such a situation would enable the financial institution to make the disclosure to the third party without first providing the initial notice required by section 248.4 or the opt out notice required by section 248.7, but the disclosure must not exceed the purposes for which consent was given. The example also states that a consumer may revoke consent at any time by exercising the right to opt out of future disclosures. We invite comment on whether safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion. Such safeguards might include, for instance, a requirement that consent be written or that it be indicated on a separate line in a relevant document or on a distinct Web page.

Section 248.12 Limits on Redisclosure and Reuse of Information

Section 248.12 of the proposed rules implements the Act's limitations on redisclosure and reuse of nonpublic personal information about consumers. Section 502(c) of the Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not, directly or indirectly through an affiliate, disclose the information to any person that is not affiliated with either the financial institution or the third party, unless the disclosure would be lawful if made directly by the financial institution. Paragraph (a)(1) sets out the Act's redisclosure limitation as it applies to a financial institution that receives information from another nonaffiliated financial institution. Paragraph (b)(1) mirrors the provisions of paragraph (a)(1), but applies the redisclosure limits to any nonaffiliated third party that receives nonpublic personal information from a financial institution.

The Act appears to place the institution that receives the information into the shoes of the institution that disclosed the information for purposes of determining whether redisclosures by the receiving institution are ''lawful.'' Thus, the Act appears to permit the receiving institution to redisclose the information to (i) an entity to whom the original transferring institution could disclose the information pursuant to one of the exceptions in section 248.9, 248.10, or 248.11, or (ii) an entity to whom the original transferring institution could have disclosed the information as described under its notice of privacy policies and practices, unless the consumer has exercised the right to opt out of that disclosure. Because a consumer can exercise the right to opt out of a disclosure at any time, the Act may effectively preclude third parties that receive information to which the opt out right applies from redisclosing the information, except under one of the exceptions in section 248.9, 248.10, or 248.11. We invite 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.

Sections 502(b)(2) and 502(e) (as implemented by sections 248.9, 248.10, and 248.11 of the proposed rules) describe when a financial institution may disclose nonpublic personal information without providing the consumer with the initial privacy notice and an opportunity to opt out, but those exceptions apply only when the information is used for the specific purposes set out in those sections. Paragraph (a)(2) of proposed section 248.12 clarifies this limitation on reuse as it applies to financial institutions. Paragraph (a)(2) provides that a financial institution may use nonpublic personal information about a consumer that it receives from a nonaffiliated financial institution in accordance with an exception under section 248.9, 248.10, or 248.11 only for the purpose of that exception. Paragraph (b)(2) applies the same limits on reuse to any nonaffiliated third party that receives nonpublic personal information from a financial institution. The example in (b)(3) clarifies that a nonaffiliated transfer agent who receives nonpublic personal information from a financial institution may not directly or indirectly disclose the information to a nonaffiliated third party of the institution and the transfer agent unless the institution could lawfully share the information with that party.

We invite comments on the meaning of the word ''lawful'' as that term is used in section 502(c). We specifically solicit comment on whether it would be lawful for a nonaffiliated third party to disclose information under the exception provided in proposed section 248.9 of the rules. Under that exception, a financial institution must comply with certain requirements before disclosing information to a nonaffiliated third party. Given that the statute and proposed rules impose those requirements on the financial institution that makes the initial disclosure, we invite comment on whether subsequent disclosures by the third party could satisfy the requirement that those disclosures be lawful when the financial institution is not party to the subsequent disclosure.

Section 248.13 Limits on Sharing of Account Number Information for Marketing Purposes

Section 502(d) of the G–L–B Act prohibits a financial institution from disclosing, other than to a consumer reporting agency, account numbers or similar forms of access numbers or access codes 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 marketing through electronic mail to the consumer. Proposed section 248.13 applies this statutory prohibition to disclosures made directly or indirectly by a financial institution.

We note that there is no exception in Title V to the flat prohibition established by section 502(d). The conference report for the G–L–B Act encourages the Commission (and the Agencies) to adopt an exception to section 502(d) to permit disclosures of account numbers in limited circumstances. It states:

> In exercising their authority under section 504(b) [which vests the Agencies with authority to grant exceptions to section 502(a)–(d) beyond those set out in the statute], the agencies and authorities described in section 504(a)(1) may consider it consistent with the purposes of this subtitle to permit the disclosure of customer account numbers or similar forms of access numbers or access codes in an encrypted, scrambled, or similarly coded form, where the disclosure is expressly authorized by the customer and is necessary to service or process a transaction expressly requested or authorized by the customer. [47]

We have not proposed an exception to the prohibition of section 502(d) because of the risks associated with third parties' direct access to a consumer's account. We seek comment

[47] H. Rep. No. 434, 106th Cong., 1st Sess. at 173 (1999).

on whether an exception to the section 502(d) prohibition that permits third parties access to account numbers is appropriate, the circumstances under which an exception would be appropriate, and how such an exception should be formulated to provide consumers with adequate protection. In addition, we invite comment on whether a consumer ought to be able to consent to the disclosure of his or her account number, notwithstanding the general prohibition in section 502(d) and, if so, what standards should apply. We also seek comment on whether section 502(d) prohibits the disclosure by a financial institution to a marketing firm of encrypted account numbers if the financial institution does not provide the marketer the key to decrypt the number.

Section 248.14 Protection of Fair Credit Reporting Act

Paragraph (c) of section 506 states that, except for the amendments noted regarding rulemaking authority, nothing in Title V 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 implements section 506(c) of the G–L–B Act by restating the statute, making only minor clarifying changes.

Section 248.15 Relation to State Laws

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

Proposed section 248.15 is substantively identical to section 507, noting that the proposed rules (like the statute) do not preempt State laws that provide greater protection for consumers than does the regulation.

Section 248.16 Effective Date; Transition Rule

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

Proposed section 248.16(a) provides an effective date of November 13, 2000. This provision is premised on adoption of a final rule within the time frame prescribed by section 504(a)(3). We intend to provide at least six months after the adoption of a final rule for financial institutions to bring their policies and procedures into compliance with the requirements of the final rule. We invite comment on whether six months after adoption of final rules is sufficient to enable financial institutions to comply with the rules.

Proposed section 248.16(b) provides a transition rule for consumers who were customers as of the effective date of the rules. Since those customer relationships already will have been established as of the rules' effective date (thereby making it inappropriate to require a financial institution to provide those customers with a copy of the institution's initial notice at the time of establishing a customer relationship), the rules require instead that the initial notice be provided within 30 days of the effective date. We invite comment on whether 30 days is enough time to permit a financial institution to deliver the required notices, bearing in mind that the G–L–B Act contemplates at least a six-month delayed effective date from the date the rules are adopted.

If a financial institution intends to disclose nonpublic personal information about someone who was a consumer before the effective date, the institution must provide the notices required by sections 248.4 and 248.7 and provide a reasonable opportunity to opt out before the effective date. If, in this instance, the institution already is disclosing information about such a consumer, it may continue to do so without interruption until the consumer opts out, in which case the institution must stop sharing nonpublic personal information about that consumer with nonaffiliated third parties as soon as reasonably practicable. We request comment on whether the proposed rule should specify a time within which the institution must stop sharing information, and if so, what the time period should be.

Section 248.30 Procedures To Safeguard Customer Information and Records

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. Proposed section 248.30 implements this section by requiring every broker, dealer, investment company, and registered investment 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.

We have not prescribed specific policies or procedures that financial institutions must adopt. Rather, we believe it more appropriate for each institution to tailor its policies and procedures to its own systems of information gathering and transfer and the needs of its customers. We request comment on whether the proposed standards should be more specific, and if so, what specifications would be appropriate for particular financial institutions.

III. General Request for Comments

The Commission requests comment on the proposed rules and suggestions for additional examples that may be appropriate to include in the rules. We also solicit comment on whether the inclusion of examples in this part is appropriate. Are there alternative methods to offer guidance of the concepts furnished by the examples?

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996,[48] we also request information regarding the potential effect of the proposals on the U.S. economy on an annual basis. Commenters are requested to provide empirical data to support their views.

The Commission strives to draft its rules according to principles outlined in its Plain English Handbook.[49] We invite your comments on how to make the proposed rule more consistent with those principles and easier to understand.

[48] Pub. L. No. 104–121, Title II, 110 Stat. 857 (1996).

[49] Office of Investor Education and Assistance, U.S. Securities and Exchange Commission, A Plain English Handbook (1998) (available on the Commission's web site at <http://www.sec.gov>).

IV. Cost-Benefit Analysis

The Commission is sensitive to the costs and benefits that result from its rules and understands that the proposed rules may impose costs on brokers, dealers, investment companies, and registered investment advisers. Nevertheless, the proposed 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 proposed 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 proposed requirements to provide initial and annual notices will allow customers to compare the privacy policies of financial institutions.

We also believe that the proposed rules will 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 proposed by the Agencies. The examples in the proposed rules also should provide guidance on how the rules will be enforced with respect to brokers, dealers, investment companies, and registered investment advisers. Finally, in order to reduce compliance burdens, the proposed rules would allow financial institutions 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.

We estimate that approximately 5500 broker-dealers, 4300 investment companies and 8100 registered investment advisers would be required to comply with the proposed rules. In the first year after the rules are adopted, these institutions would be required to comply with the following requirements: (i) Prepare notices describing the institution's privacy policies; (ii) provide an initial privacy notice and opt out form 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, institutions would be required to revise notices only to reflect changes in their privacy policies. Similarly, institutions would have to revise their policies and procedures on safeguarding customer information as appropriate to ensure the protection of the information.

Under the proposed rules, an initial and annual notice could be the same.[50] Many broker-dealers, investment companies, and registered investment advisers currently provide notice of their privacy policies to consumers and customers.[51] Thus, some of these institutions would be required to draft privacy notices, while others would have to review and revise their notices for compliance with the proposed rules.

The amount of time required for each institution to prepare (or revise) its privacy policy 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.[52] We assume that while broker-dealers and investment companies share nonpublic personal information about consumers or customers with their affiliates (or as permitted under one of the exceptions discussed above), few, if any, share information with nonaffiliated third parties.[53] In addition, we assume that most investment advisers do not share the information with any third parties.[54] Based on these assumptions, we estimate that an investment adviser would require, on average, about 5 hours, and a broker-dealer or investment company would require from 5 to over 100 hours, with an average of about 40 hours, to prepare (or revise) its privacy notice. Assuming that an investment adviser would spend on average $615 [55] to draft a notice, and a broker-dealer or investment company would spend on average $4920,[56] we estimate that the total one-time cost to the industry of drafting privacy notices would be approximately $53.2 million.[57]

As noted above, we assume that broker-dealers, investment companies, and registered investment advisers do not share nonpublic personal information with nonaffiliated third parties. Therefore, those institutions would not be required to provide consumers an initial notice or opportunity to opt out. We assume that those institutions generally will include initial and annual privacy notices to customers with disclosure documents or account statements that they currently receive.[58] These statements generally are assembled and sent by organizations that specialize in mailing and distribution. We estimate that the additional material might result in an increase in total annual distribution costs of $2.6 million for broker-dealers, investment companies, and registered investment advisers.[59]

We understand that most if not all broker-dealers, investment companies, and registered investment advisers have established some policies and procedures to protect customer information.[60] Each institution,

[50] *See* proposed § 248.6(a) (specifying the same content for initial and annual notices).

[51] *See e.g.,* Charles Schwab & Co., The Schwab Privacy Pledge & Notification (Sept. 23, 1999) (available at <http://www.schwab.com>); The Vanguard Group, Privacy Policy (available at <http://www.vanguard.com>).

[52] An institution that does not share information with affiliates or nonaffiliated third parties may simply state that fact without further discussion. *See* discussion regarding proposed section 248.6 above. 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.

[53] This assumption is based on staff conversations with representatives of the securities industry.

[54] *See* Association for Investment Management and Research, Standards of Practice Handbook 123, 125 (1996) (standard requires members to preserve the confidentiality of information communicated by clients or prospects, and procedures for compliance explain the ''simplest, most conservative, and most effective'' way to comply is to avoid disclosing any information received from a client except to authorized fellow employees who also work for the client).

[55] 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).

[56] 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).

[57] This amount equals the sum of the costs for broker-dealers, investment companies, and investment advisers ((5500 + 4300) × $4920) + (8,100 × $615) = $53.2 million.

[58] Some customers receive all their correspondence electronically and could receive notices through the same medium. We believe that institutions would incur only minimal costs in transmitting notices to these customers electronically.

[59] The individual cost per institution would vary significantly depending on the number of the institution's customers. The estimate is based on an average additional cost per mailing of $0.02 for 130.7 million investor accounts. The number of investor accounts assumes there are 53 million brokerage accounts, 77.3 million individual investment company shareholders (*see* Investment Company Institute, 1999 Mutual Fund Fact Book 41 (May 1999)), and 400,000 customers of investment advisers. The estimated number of accounts may be significantly higher than the actual number because we are unable to estimate the number of individual accounts used for personal, family, or household purposes. *See* proposed § 248.1(b).

[60] *See* Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Securities Act Release No. 7288 (May 9, 1996) [61 FR 24644, 24647 (May 15, 1996)] (advising broker-dealers, transfer agents, and investment advisers to take reasonable precautions to ensure the integrity, confidentiality, and security of information about a customer's personal financial matters, and to tailor those precautions to the medium used (whether electronic means or paper) to ensure the information is reasonably secure from

however, would be likely to review and, as appropriate, revise its protection policies to assure compliance with the proposed rules. Assuming that each institution will on average require approximately 30 hours to review and revise its policies and procedures, the one-time cost to the industry to comply with the rules would be approximately $80.6 million.[61]

As discussed above, the privacy notices will allow customers of broker-dealers, investment companies, and registered investment 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 customer's 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, investment companies, 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.

We request comment on the costs and benefits of the proposed rules. We specifically request comment on the anticipated costs of drafting or revising privacy notices. We also request comment on the extent to which broker-dealers, investment companies, and registered investment advisers have established policies to protect customer information and the extent to which those policies would have to be revised to comply with the proposed rules. We invite comment on the cost of including privacy notices in other mailings, as well as the proportion of individual account holders who may receive notices electronically and the resulting costs or savings.

V. Paperwork Reduction Act

Certain provisions of the proposed rules contain ''collection of information'' requirements within the meaning of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*). The Commission has submitted these provisions to the Office of Management and Budget (''OMB'') for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. The title for the collections of information is: ''Regulation S–P.'' 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.

Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comment to:

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

(2) Evaluate the accuracy of the Commission's estimate of the burden of the proposed collections of information;

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

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

The proposed rules contain several disclosure requirements. The financial institutions must prepare and provide an initial notice to all current customers and all new customers at the time of establishing a customer relationship.[62] Subsequently, an annual notice must be provided to all customers at least once during a twelve-month period during the continuation of the customer relationship.[63] The initial notice and opt out notice must be provided to a consumer prior to disclosing nonpublic personal information to certain nonaffiliated third parties.[64] If a financial institution wishes to disclose information in a way that is inconsistent with the notices previously given to a consumer, the financial institution must provide consumers with revised notices (proposed § 248.8(c)).

The proposed regulation also contains consumer reporting requirements. In order for consumers to opt out, they must respond to the opt out notice.[65] At any time during their continued relationship, consumers have the right to change or update their opt out status.[66] As discussed above, we believe that most, if not all, financial institutions will not share nonpublic personal information about consumers with nonaffiliated third parties and will not have to provide opt out notices to consumers or customers. Thus, few, if any, consumers will need to respond to opt out notices. The Commission therefore estimates that the annual burden of responding to an opt out notice will be nominal. The Commission requests public comment on all aspects of the collections of information contained in this proposed regulation, including consumer responses to the opt out notice and consumer changes to their opt out status with a financial institution.

The initial and annual privacy notices are mandatory. The opt out notice is not mandatory for institutions that do not share nonpublic personal information with nonaffiliated third parties. The likely respondents are brokers, dealers, investment companies, and registered investment advisers. The required notices are not submitted to the Commission, and there is no assurance of confidentiality of the collections of information. The Commission estimates that approximately 5500 broker-dealers, 4300 investment companies, and 8100 registered investment advisers will respond to the proposed regulation.

Estimated average annual burden hours per respondent: 40.

Estimated average annual dollar burden per respondent: $145.00.[67]

Estimated number of respondents: 17,900.

Estimated total annual hour burden: 716,000 hours.

Estimated total annual dollar burden: $2.6 million.

Persons desiring to submit comments on the collection of information requirements should direct them to the Office of Management and Budget, Attention: Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Washington, DC 20503, and should also send a copy to Jonathan G. Katz, Secretary, Securities and Exchange Commission, 450 Fifth Street, NW, Washington, DC 20549 with reference to File No. S7–6–00. OMB is required to make a decision concerning the collection of information between 30 and 60 days after publication, so a comment to OMB is best assured of having its full effect if OMB receives it

tampering or alteration); Investment Company Institute, Protection of Data Privacy in the Investment Company Industry (June 22, 1998) (available at <http://www.ici.org>) (investment companies and their managers often have written policies to ensure confidentiality of customer information).

[61] This estimate represents the costs of 30 hours of professional time (at $150 per hour) ((5500 + 4300 + 8100) × 30 × $150 = $80.6 million). Our estimates are 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.

[62] Proposed § 248.4(a).

[63] Proposed § 248.5(a).

[64] Proposed §§ 248.7(a)(1)(i) and (ii).

[65] Proposed §§ 248.7(a)(2), (a)(3)(i), (c).

[66] Proposed §§ 248.8(d) and (e).

[67] This amount represents an estimated annual cost to include privacy notices in account statements or shareholder reports sent to customers.

within 30 days after publication. Requests for materials submitted to OMB by the Commission with regard to this collection of information should be in writing, refer to File No. S7–6–00, and be submitted to the Securities and Exchange Commission, Records Management, Office of Filings and Information Services, 450 5th Street, NW, Washington, DC 20549.

VI. Summary of Initial Regulatory Flexibility Analysis

The Commission has prepared an Initial Regulatory Flexibility Analysis (''IRFA'' or ''analysis'') for proposed Regulation S–P in accordance with 5 U.S.C. 603. The following summarizes the IRFA. A copy of the IRFA may be obtained by contacting Penelope W. Saltzman, Securities and Exchange Commission, 450 5th Street, NW, Washington, DC 20549–0506.

The analysis explains 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 explains that subject to certain exceptions, the proposed rules generally require that a financial institution provide all of its *customers* the following notices: (i) An initial privacy notice (before the customer relationship is established or, for existing customers, within 30 days after the rule's effective date); (ii) an opt out notice (before sharing the individual's nonpublic personal information with nonaffiliated third parties); and (iii) an annual privacy notice for the duration of the customer relationship.

The proposed 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 such information about its consumers, then it need not provide a privacy or opt out notice.

The many exceptions to the general rules stated above are set forth in proposed sections 248.9, 248.10, and 248.11. 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 must 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 a majority of financial institutions already have privacy policies in place as part of usual and customary business practices.[68] We have estimated that a financial institution would spend approximately 40 hours on average to prepare the privacy notices.

To minimize the burden and costs of distributing privacy policies, the proposed rule does 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 notes that we understand that most, if not all, brokers, dealers, investment companies, 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 proposed rules. 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 proposed rules, most if not all financial institutions will not have to provide opt out notices to consumers or customers, and will not need to revise their contracts with nonaffiliated third parties to restrict those parties' use of information.

The analysis explains that the proposed rule requires every broker, dealer, investment company, and registered investment adviser to adopt policies and procedures reasonably designed to safeguard customer records and information. We 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. We have estimated that in the first year after the proposed rules are adopted, a financial institution would spend an average of 30 hours to adopt or revise its policies.

The proposed rules would affect all brokers, dealers, investment companies, and registered investment advisers, including small entities.[69] We estimate

[68] For example, investment advisers have fiduciary duties under state law that limit the ability of an investment adviser to share information with third parties. *See supra* note 4. This and other assumptions discussed in this paragraph also are based on staff conversations with representatives from the securities industry.

[69] For purposes of the Regulatory Flexibility Act, under the Exchange Act a small entity is a broker

that approximately 1000 out of 5500 brokers and dealers, 227 out of 4300 investment companies, and 1500 out of 8,100 registered investment advisers are small entities.

As noted in the analysis, the scope of the proposed regulation (pursuant to the G–L–B Act) is unique. Nevertheless, as discussed in greater detail in the analysis, there may be some overlap in certain circumstances with certain federal laws.

The analysis explains that the Reg. Flex. Act directs the Commission to consider significant alternatives that would accomplish the stated objective, while minimizing any significant adverse impact on small entities. In addition to clarifying and simplifying the statutory requirements for all financial institutions, the proposed rule also provides substantial flexibility so that any financial institution, regardless of size, may tailor its practices to its individual needs. As discussed more fully in the analysis, we believe that an exception that would create different levels of protections for consumers based on the size of the institution with which they conduct business would not be consistent with the purposes of Title V. The Commission welcomes comment on any significant alternatives, consistent with the G–L–B Act, that would minimize the impact on small entities.

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

Section 23(a)(2) of the Exchange Act[70] requires the Commission, in adopting rules under the Exchange Act, to consider the anti-competitive effects of any rules it adopts. We do not believe that the proposed rules will result in anti-competitive effects. The proposed rules, which implement Title V, apply to all broker-dealers, investment companies, and registered investment advisers. Each of these institutions would be required to provide initial and annual privacy notices to customers as well as initial notices and opt out forms to consumers if the institution shares nonpublic personal information about consumers with nonaffiliated third parties. These institutions also would be required to 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 proposed by other federal agencies.[71] Under the G–L–B Act, these agencies also are required to adopt rules addressing policies and procedures for protecting customer information.[72] Therefore, all financial institutions will have to bear the costs of implementing the proposed rules or substantially similar rules. Although these costs will vary among institutions, we do not believe that the costs will be significantly greater (as a proportion of the institutions' costs) for any particular institutions.

As noted above, some customers may move their accounts from one institution to another based on the institution's privacy policies. Thus, the proposed rules may promote competition among financial institutions based on customers' preferences regarding privacy policies. The rules do not, however, dictate the privacy policies of any financial institution. We have no basis for estimating the circumstances under which customers may move accounts. Thus, we cannot measure the potential benefits to competition or predict whether there may be anti-competitive effects with respect to institutions based on their privacy policies. We request comment on any anti-competitive effects of the proposed rules.

Section 3(f) of the Exchange Act,[73] and section 2(c) of the Investment Company Act[74] 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. Our analysis on competition is discussed above. We believe the proposed rules will have little effect on efficiency and capital formation. We have estimated that the proposed rules will result in additional costs for financial institutions. Nevertheless, we believe the additional costs are small enough that they will not affect the efficiency of these institutions. 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. This may result in greater efficiencies if customers make this choice before doing business with an institution instead of having to close an account after learning that an institution shares information in ways the customer does not want. We have no basis, however, for estimating the extent of these potential efficiencies. We request comment on these matters in connection with the proposed rule.

VIII. Statutory Authority

The Commission is proposing 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].

List of Subjects in 17 CFR Part 248

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

Text of Proposed Rules

For the reasons set out in the preamble, the Commission proposes to amend 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.

or dealer that had total capital of less than $500,000 on the date of its prior fiscal year 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.

[70] 15 U.S.C. 78w(a)(2).

[71] *See, e.g.,* Banking Agencies' Proposal, *supra* note 2.

[72] G–L–B Act § 501(b).

[73] 15 U.S.C. 78c(f).

[74] 15 U.S.C. 80a–2(c).

Authority: 15 U.S.C. 6801–6809; 15 U.S.C. 78q, 78w, 80a–30(a), 80a–37, 80b–4, 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 consumers about its privacy policies and practices;

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

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 248.9, 248.10, and 248.11.

(b) *Scope.* The rules established by this part apply only to nonpublic personal information about individuals who obtain financial products or services for personal, family or household purposes from the institutions listed in section 248.3(x). This part does not apply to information about companies or about individuals who obtain financial products or services for business purposes. This part applies to brokers, dealers, and investment companies and to investment advisers that are registered with the Commission. These entities are referred to in this part as ''you.''

§ 248.2 Rule of construction.

The examples in 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 constitutes compliance with the applicable rule.

§ 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 a government regulator other than the Commission; and

(2) Rules adopted by the other government 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 contained in the notice.

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

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

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

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

(D) Avoid multiple negatives;

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

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

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

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

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

(C) Provide wide margins and ample line spacing.

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

(A) Larger type size(s);

(B) Boldface or italics for key words in the text;

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

(D) Shading or sidebars to highlight the notice.

(d) *Collect* means to obtain information that is organized or retrievable on a personally identifiable basis, 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, and that individual's legal representative.

(2) *Examples.* (i) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain brokerage services or investment advisory services is a consumer whether or not you provide brokerage services to the individual or establish an ongoing advisory relationship with the individual.

(ii) An individual who provides you with name, address, and areas of investment interest in connection with a request for a prospectus or an investment adviser brochure or other information about financial products is not a consumer.

(iii) An individual is not a consumer for your purposes when the individual has an account with another broker or dealer that carries securities for the individual in a special omnibus account with you in the name of the broker or dealer, and when you do not routinely receive any information about the consumer.

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

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

(A) Has a brokerage account with you;

(B) Has an investment advisory contract with you (whether written or oral); or

(C) Is the record owner of securities you have issued if you are an investment company.

(ii) You have a customer relationship with a consumer if the consumer has an account with an introducing broker-dealer that clears transactions with and for its customers through you on a fully disclosed basis.

(iii) You have a customer relationship with a consumer if 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.

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

(v) A consumer who does not establish an account with you does not have a continuing relationship with you if you provide brokerage services to the consumer on a one-time basis as an accommodation or to liquidate securities 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)(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.

(n)(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, brokerage or distribution of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(3) *Financial product,* for purposes of this part, includes an equity interest in an investment company.

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

(p) *Government regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission;

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

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

(9) The Federal Trade Commission.

(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 by virtue of the direct or indirect ownership or control of the company by the financial institution or any affiliate of the financial institution in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(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 about them) that is derived using any personally identifiable financial information.

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

(i) Publicly available information, except as provided in paragraph (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 customer; or

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

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

(u) *Person* has the same meaning as in section 3(a)(9) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(9)).

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

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

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

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

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

(A) Information a consumer provides to you on an application to establish a brokerage account, enter into an investment advisory contract, or to purchase securities or other financial products or services, including, among other things, medical information;

(B) Information about account balance, payment history, overdraft history, credit or debit card purchases,

securities positions, or investment products purchased or sold;

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

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

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

(F) Information from a consumer report.

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

(w)(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) *Government records.* Publicly available information contained in government records includes information contained in government real estate records, security interest filings, and bankruptcy filings.

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

(x) *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.

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

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

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

(2) A consumer (who has not become your customer), prior to the time that you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 248.10 and 248.11.

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

(1) You do not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by §§ 248.9, 248.10, or 248.11; and

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

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

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

(2) *Exceptions to allow subsequent delivery of notice.* You may provide the initial notice required by paragraph (a) of this section within a reasonable time after you establish a customer relationship if you and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice thereafter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 248.5 Annual notice to customers required.

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

(b) *How to provide notice.* You must provide the annual notice required by paragraph (a) of this section to a

customer using a means permitted for providing the initial notice to that customer under § 248.4(d).

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

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

(i) 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 no longer holds shares in the company; 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).

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

(a) *General rule.* The initial and annual notices that you provide about your privacy policies and practices under §§ 248.4 and 248.5 must include each of the following items of information:

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your consumers, other than those parties to whom you disclose information under §§ 248.10 (exceptions for processing and servicing accounts or transactions) and 248.11 (exceptions for consumer consent and to comply with various legal requirements);

(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 §§ 248.10 and 248.11;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 248.9 (and no other exception applies to that disclosure), a separate description of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the right under § 248.8(a) of the consumer to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;

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

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

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information about a consumer to third parties as authorized under §§ 248.10 and 248.11, 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 only required to state that you make disclosures to other nonaffiliated third parties as permitted by law.

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

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

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

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

(2) *Categories of nonpublic personal information you disclose.* You adequately categorize nonpublic personal information you disclose if you categorize it according to source, and provide a few illustrative examples of the content of the information. These might include application information, such as assets and income, investment goals, or investment risk tolerance; identifying information, such as name, address, and social security number; and transaction information, such as information about account balance, payment history, parties to the transaction, credit card usage, securities positions, or securities purchases and sales; and information from consumer reports, such as a consumer's creditworthiness and credit history. You do not adequately categorize the information that you disclose if you use only general terms, such as transaction information about the consumer.

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

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

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

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

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

(i) You have provided to the consumer an initial notice as required under § 248.4;

(ii) You have provided to the consumer an opt out notice as required in § 248.8;

(iii) You have given the consumer a reasonable opportunity, before the time

that you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 248.9, 248.10 and 248.11.

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

(ii) *Isolated transaction with consumer.* For an isolated transaction, such as the provision of brokerage services as an accommodation to a consumer who does not establish an account with you, you provide a reasonable opportunity to opt out if you provide the consumer with the required notices at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

(b) *Application of opt out to all consumers and all nonpublic personal information.*

(1) 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.

§ 248.8 Form and method of providing opt out notice to consumers.

(a)(1) *Form of opt out notice.* You must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under § 248.7(a)(1). The notice must state:

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

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

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

(2) *Examples.* (i) You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose to nonaffiliated third parties as described in § 248.6 and state that the consumer can opt out of the disclosure of that information.

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

(A) Designate check-off boxes in a prominent position on the relevant forms with the opt out notice;

(B) Include a reply form together with the opt out notice; or

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

(iii) You do not provide a reasonable means of opting out if the only means of opting out is for the consumer to write his or her own letter to exercise that opt out right.

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

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

(3) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 248.4.

(4) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice at a later time than required for the initial notice in accordance with § 248.4, you must also include a copy of the initial notice in writing or, if the consumer agrees, in an electronic form with the opt out notice.

(c) *Notice of change in terms.* (1) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to the consumer under § 248.4, unless:

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

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

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

(iv) The consumer does not opt out.

(2) *How to provide notice of change in terms.* You must provide the revised notice of your policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under § 248.4(d) or § 248.8(b).

(3) *Examples.* (i) Except as otherwise permitted by §§ 248.9, 248.10 and 248.11, a change-in-terms notice is required if you:

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

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

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

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

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

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

(a) *General rule.* The opt out requirements in §§ 248.7 and 248.8 do not apply when you provide nonpublic personal information about a consumer to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(1) Provide the initial notice in accordance with § 248.4; and

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

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

(ii) Limits the third party's use of information you disclose solely to the purposes for which the information is disclosed or as otherwise permitted by §§ 248.10 and 248.11.

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

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

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

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 248.4(a)(2), the opt out in §§ 248.7 and 248.8, and service providers and joint marketing in § 248.9, do not apply if you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 248.11 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice to consumers in § 248.4(a)(2), the opt out in §§ 248.7 and 248.8, and initial notice to consumers under the exception for service providers and joint marketing in § 248.9, do not apply when you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

(7)(i) To comply with federal, State, or local laws, rules and other applicable legal requirements, including rules or other applicable legal requirements of self-regulatory organizations;

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

(iii) To respond to judicial process, government regulatory authorities, or self-regulatory organizations 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 § 248.8(d).

§ 248.12 Limits on redisclosure and reuse of information.

(a) *Limits on your redisclosure and reuse.* (1) Except as otherwise provided in this part, if you receive nonpublic personal information about a consumer from a nonaffiliated financial institution, you must not, directly or through an affiliate, disclose the

information to any other person that is not affiliated with either the financial institution or you, unless the disclosure would be lawful if the financial institution made it directly to that other person.

(2) You may use nonpublic personal information about a consumer that you receive from a nonaffiliated financial institution in accordance with an exception under §§ 248.9, 248.10, or 248.11 only for the purpose of that exception.

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

(2) A nonaffiliated third party may use nonpublic personal information about a consumer that it receives from you in accordance with an exception under §§ 248.9, 248.10, or 248.11 only for the purpose of that exception.

(3) *Example.* If you provide nonpublic personal information to a nonaffiliated transfer agent that services your customer accounts, the transfer agent may not, directly or through an affiliate, disclose the nonpublic personal information to any other person that is a nonaffiliated third party of you and the transfer agent unless you could lawfully make the disclosure to that party.

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

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

§ 248.14 Protection of Fair Credit Reporting Act.

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

§ 248.15 Relation to State laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that the 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 that 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.

§ 248.16 Effective date; transition rule.

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

(b) *Notice requirement for consumers who were your customers on the effective date.* No later than thirty days after the effective date of this part, you must provide an initial notice, as required by § 248.4, to consumers who were your customers on the effective date of this part.

§§ 248.17–248.29 [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.

By the Commission.

Dated: March 2, 2000.

Margaret H. McFarland,

Deputy Secretary.

[FR Doc. 00–5526 Filed 3–3–00; 10:05 am]

BILLING CODE 8010–01–P