year commencing after September 30, 2008.

PART 248—REGULATIONS S–P, S–AM, AND S–ID

Subpart A—Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information

Subpart B—Regulation S-AM: Limitations on Affiliate Marketing

Subpart C—Regulation S–ID: Identity Theft Red Flags

AUTHORITY: 15 U.S.C. 78q, 78q-1, 78*o*-4, 78*o*-5, 78w, 78mm, 80a-30, 80a-37, 80b-4, 80b-11, 1681m(e), 1681s(b), 1681s-3 and note, 1681w(a)(1), 6801–6809, and 6825; Pub. L. 111–203, secs. 1088(a)(8), (a)(10), and sec. 1088(b), 124 Stat. 1376 (2010).

SOURCE: 65 FR 40362, June 29, 2000, unless otherwise noted.

EDITORIAL NOTE: Nomenclature changes to part 248 appear at 74 FR 40431, Aug. 11, 2009.

Subpart A—Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information

§ 248.1 Purpose and scope.

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

(1) Requires a financial institution to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information

about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 248.13, 248.14, and 248.15.

(b) *Scope.* Except with respect to § 248.30(b), this subpart applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below. This subpart does not apply to information about companies or about individuals who obtain financial products or services primarily for business, commercial, or agricultural purposes. This part applies to brokers, dealers, and investment companies, as well as to investment advisers that are registered with the Commission. It also applies to foreign (non-resident) brokers, dealers, investment companies and investment advisers that are registered with the Commission. These entities are referred to in this subpart as ''you.'' This subpart does not apply to foreign (non-resident) brokers, dealers, investment companies and investment advisers that are not registered with the Commission. Nothing in this subpart modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–1320d–8).

[65 FR 40362, June 29, 2000, as amended at 69 FR 71329, Dec. 8, 2004]

§ 248.2 Model privacy form: rule of construction.

(a) *Model privacy form.* Use of the model privacy form in appendix A to subpart A of this part, consistent with the instructions in appendix A to subpart A, constitutes compliance with the notice content requirements of §§ 248.6 and 248.7 of this part, although use of the model privacy form is not required.

(b) *Examples.* 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, to the extent practicable, constitutes compliance with this part.

(c) *Substituted compliance with CFTC financial privacy rules by futures commission merchants and introducing brokers.* Except with respect to § 248.30(b), any futures commission merchant or introducing broker (as those terms are defined in the Commodity Exchange Act (7 U.S.C. 1, *et seq.*)) registered by notice with the Commission for the purpose of conducting business in security futures products pursuant to section 15(b)(11)(A) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)(A)) that is subject to and in compliance with the financial privacy rules of the Commodity Futures Trading Commission (17 CFR part 160) will be deemed to be in compliance with this part.

[74 FR 62984, Dec. 1, 2009]

§ 248.3 Definitions.

As used in this subpart, 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 subpart if:

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

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

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

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

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

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

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

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

(D) Avoid multiple negatives;

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

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

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

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

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

(C) Provide wide margins and ample line spacing;

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

(E) Use distinctive type size, style, and graphic devices, such as shading or sidebars when you combine your notice with other information.

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

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

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

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

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

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

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

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

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

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

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

(v) An individual who is a consumer of another financial institution is not

your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(m) *Federal functional regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board

(6) The Securities and Exchange Commission; and

(7) The Commodity Futures Trading Commission.

(n)(1) *Financial institution* means any institution the business of which is engaging in activities that are financial

in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) *Financial institution* does not include:

(i) 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

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

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

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

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

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

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

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

(i) Your affiliate; or

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

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

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

(i) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information.

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

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

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available information.

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

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

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

(i) A consumer provides to you to obtain a financial product or service from you;

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

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

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

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

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

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

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

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

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

(G) Information from a consumer report.

(ii) *Information not included.* Personally identifiable financial information does not include:

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

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

(v)(1) *Publicly available information* means any information that you reasonably believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

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

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

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

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

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

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

(iii) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(w) *You* means:

(1) Any broker or dealer;

(2) Any investment company; and

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

[65 FR 40362, June 29, 2000, as amended at 66 FR 45147, Aug. 27, 2001; 74 FR 40431, Aug. 11, 2009]

PRIVACY AND OPT OUT NOTICES

§ 248.4 Initial privacy notice to consumers required.

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

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

(2) *Consumer.* A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 248.14 and 248.15.

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

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 248.14 and 248.15; and

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

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

(2) *Special rule for loans.* You do not have a customer relationship with a consumer if you buy a loan made to the consumer but do not have the servicing rights for that loan.

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

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

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

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

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

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

(1) You may provide a revised privacy notice, under § 248.8, that covers the customer's new financial product or service; or

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

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

(i) Establishing the customer relationship is not at the customer's election;

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

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

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

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

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

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

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

§ 248.5 Annual privacy notice to customers required.

(a)(1) *General rule*. Except as provided by paragraph (e) of this section, you must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

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

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

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

(i) The individual's brokerage account is closed;

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

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

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

(c) *Special rule for loans.* If you do not have a customer relationship with a consumer under the special provision for loans in § 248.4(c)(2), then you need not provide an annual notice to that consumer under this section.

(d) *Delivery*. When you are required to deliver an annual privacy notice by this section, you must deliver it according to § 248.9.

(e) *Exception to annual privacy notice requirement*—(1) *When exception available.* You are not required to deliver an annual privacy notice if you:

(i) Provide nonpublic personal information to nonaffiliated third parties only in accordance with § 248.13, § 248.14, or § 248.15; and

(ii) Have not changed your policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 248.6(a)(2) through (5) and (9) in the most recent privacy notice provided pursuant to this part.

(2) *Delivery of annual privacy notice after financial institution no longer meets the requirements for exception*. If you have been excepted from delivering an annual privacy notice pursuant to paragraph (e)(1) of this section and change your policies or practices in such a way that you no longer meet the requirements for that exception, you must comply with paragraph (e)(2)(i) or (ii) of this section, as applicable.

(i) *Changes preceded by a revised privacy notice.* If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that § 248.8 requires you to provide a revised privacy notice, you must provide an annual privacy notice in accordance with the timing requirement in paragraph (a) of this section, treating the revised privacy notice as an initial privacy notice.

(ii) *Changes not preceded by a revised privacy notice.* If you no longer meet the requirements of paragraph (e)(1) of this section because you change your

policies or practices in such a way that § 248.8 does not require you to provide a revised privacy notice, you must provide an annual privacy notice within 100 days of the change in your policies or practices that causes you to no longer meet the requirement of paragraph (e)(1) of this section.

(iii) *Examples.* (A) You change your policies and practices in such a way that you no longer meet the requirements of paragraph (e)(1) of this section effective April 1 of year 1. Assuming you define the 12-consecutive-month period pursuant to paragraph (a) of this section as a calendar year, if you were required to provide a revised privacy notice under § 248.8 and you provided that notice on March 1 of year 1, you must provide an annual privacy notice by December 31 of year 2. If you were not required to provide a revised privacy notice under § 248.8, you must provide an annual privacy notice by July 9 of year 1.

(B) You change your policies and practices in such a way that you no longer meet the requirements of paragraph (e)(1) of this section, and so provide an annual notice to your customers. After providing the annual notice to your customers, you once again meet the requirements of paragraph (e)(1) of this section for an exception to the annual notice requirement. You do not need to provide additional annual notice to your customers until such time as you no longer meet the requirements of paragraph (e)(1) of this section.

[65 FR 40362, June 29, 2000, as amended at 89 FR 47786, June 3, 2024]

§ 248.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under §§ 248.4, 248.5, and 248.8 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§ 248.14 and 248.15;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 248.14 and 248.15;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 248.13 (and no other exception applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the consumer's right under § 248.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

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

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

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

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information to third parties as authorized under §§ 248.14 and 248.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 248.4 and 248.5. When describing the categories with respect to those parties, it is sufficient to state that you make disclosures to other nonaffiliated companies:

(1) For your everyday business purposes such as [*include all that apply*] to process transactions, maintain account(s), respond to court orders and

legal investigations, or report to credit bureaus; or

(2) As permitted by law.

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

(i) Information from the consumer;

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

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

(iv) Information from a consumer-reporting agency.

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

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

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

(i) Financial service providers;

(ii) Non-financial companies; and

(iii) Others.

(4) *Disclosures under exception for service providers and joint marketers.* If you disclose nonpublic personal information under the exception in § 248.13 to a nonaffiliated third party to market products or services that you offer alone or jointly with another financial institution, you satisfy the disclosure requirement of paragraph (a)(5) of this section if you:

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

(ii) State whether the third party is:

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

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

(5) *Simplified notices.* If you do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information to affiliates or nonaffiliated third parties except as authorized under §§ 248.14 and 248.15, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

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

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

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

(d) *Short-form initial notice with opt out notice for non-customers.* (1) You may satisfy the initial notice requirements in §§ 248.4(a)(2), 248.7(b), and 248.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in § 248.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

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

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

(3) You must deliver your short-form initial notice according to § 248.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply

provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to § 248.9.

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

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

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

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

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

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

(f) *Model privacy form.* Pursuant to § 248.2(a) and appendix A to subpart A of this part, Form S–P meets the notice content requirements of this section.

[65 FR 40362, June 29, 2000, as amended at 74 FR 62985, Dec. 1, 2009]

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

(a)(1) *Form of opt out notice.* If you are required to provide an opt out notice under § 248.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. The notice must state:

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

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

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

(2) *Examples*—(i) *Adequate opt out notice.* You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you:

(A) Identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose, and all of the categories of nonaffiliated third parties to which you disclose the information, as described in § 248.6(a)(2) and (3) and state that the consumer can opt out of the disclosure of that information; and

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

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

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

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

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

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

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

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

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

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

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

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice

after the initial notice in accordance with §248.4, you must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

(d) *Joint relationships.* (1) If two or more consumers jointly obtain a financial product or service from you, you may provide a single opt out notice. Your opt out notice must explain how you will treat an opt out direction by a joint consumer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(h) *Delivery.* When you are required to deliver an opt out notice by this section, you must deliver it according to §248.9.

(i) *Model privacy form.* Pursuant to §248.2(a) and appendix A to subpart A of this part, Form S–P meets the notice content requirements of this section.

[65 FR 40362, June 29, 2000, as amended at 74 FR 62985, Dec. 1, 2009]

§ 248.8 Revised privacy notices.

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

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

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

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

(4) The consumer does not opt out.

(b) *Examples.* (1) Except as otherwise permitted by §§248.13, 248.14, and 248.15,

you must provide a revised notice before you:

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

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

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

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

(c) *Delivery*. When you are required to deliver a revised privacy notice by this section, you must deliver it according to § 248.9.

§ 248.9 Delivering privacy and opt out notices.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(e) *Retention or accessibility of notices for customers*. (1) For customers only, you must provide the initial notice required by § 248.4(a)(1), the annual notice required by § 248.5(a), and the revised notice required by § 248.8, so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

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

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

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

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

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

(g) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from you, you may satisfy the initial, annual, and revised notice requirements of paragraph (a) of this section by providing one notice to those consumers jointly.

LIMITS ON DISCLOSURES

§ 248.10 Limits on disclosure of nonpublic personal information to nonaffiliated third parties.

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

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

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

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

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 248.13, 248.14, and 248.15.

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

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

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

(iii) *Isolated transaction with consumer.* For an isolated transaction, such as the provision of brokerage services to a consumer as an accommodation, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

(b) *Application of opt out to all consumers and all nonpublic personal information.* (1) You must comply with this section, regardless of whether you and the consumer have established a customer relationship.

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

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

§ 248.11 Limits on redisclosure and reuse of information.

(a)(1) *Information you receive under an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in § 248.14 or § 248.15, your disclosure and use of that information is limited as follows:

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

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

(iii) You may disclose and use the information pursuant to an exception in § 248.14 or § 248.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.

(2) *Example.* If you receive a customer list from a nonaffiliated financial institution in order to provide account-processing services under the exception in § 248.14(a), you may disclose that information under any exception in § 248.14 or § 248.15 in the ordinary course of business in order to provide those services. You could also disclose that information in response to a properly authorized subpoena or in the ordinary course of business to your attorneys, accountants, and auditors. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

(b)(1) *Information you receive outside of an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution other than under an exception in § 248.14 or § 248.15, you may disclose the information only:

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

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

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

(2) *Example.* If you obtain a customer list from a nonaffiliated financial institution outside of the exceptions in §§ 248.14 and 248.15:

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

(ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed the list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list, as limited by the opt out direction of each consumer whose nonpublic personal information you intend to disclose, and you may disclose the list in accordance with an exception in § 248.14 or § 248.15, such as in the ordinary course of business to your attorneys, accountants, or auditors.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal information to a nonaffiliated third party under an exception in § 248.14 or § 248.15, the third party may disclose and use that information only as follows:

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

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

(3) The third party may disclose and use the information pursuant to an exception in § 248.14 or § 248.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) *Information you disclose outside of an exception.* If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in § 248.14 or § 248.15, the third party may disclose the information only:

(1) To your affiliates;

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

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

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

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

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

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

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

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

EXCEPTIONS

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

(a) *General rule.* (1) The opt out requirements in §§ 248.7 and 248.10 do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

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

(ii) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in § 248.14 or § 248.15 in the ordinary course of business to carry out those purposes.

(2) *Example.* If you disclose nonpublic personal information under this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in § 248.14 or § 248.15 in the ordinary course of business to carry out that joint marketing.

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

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

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

(a) *Exceptions for processing and servicing transactions at consumer's request.* The requirements for initial notice in § 248.4(a)(2), for the opt out in §§ 248.7 and 248.10, and for initial notice in § 248.13 in connection with service providers and joint marketing, do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Processing or servicing a financial product or service that a consumer requests or authorizes;

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

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or

similar transaction related to a transaction of the consumer.

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

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

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

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

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

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

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

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

(vi) In connection with:

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

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

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

§ 248.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to notice and opt out requirements.* The requirements for initial notice in § 248.4(a)(2), for the opt out in §§ 248.7 and 248.10, and for initial notice in § 248.13 in connection with service providers and joint marketing do not apply when you disclose nonpublic personal information:

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

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

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

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

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

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

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

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*), to law enforcement agencies (including a federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a State insurance authority, with respect to any person domiciled in that insurance authority's State that is engaged in providing insurance, and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

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

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

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

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

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

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

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated mortgage lender of the value of the assets in the consumer's brokerage or investment advisory account so that the lender can evaluate the consumer's application for a mortgage loan.

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

RELATION TO OTHER LAWS; EFFECTIVE DATE

§ 248.16 Protection of Fair Credit Reporting Act.

Nothing in this subpart 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 subpart regarding whether information is transaction or experience information under section 603 of that Act.

§ 248.17 Relation to State laws.

(a) *In general.* This subpart shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such State statute, regulation, order, or interpretation is inconsistent with the provisions of this subpart, 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 subpart if the protection such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this subpart, as determined by the Consumer Financial Protection Bureau, after consultation with the Commission, on theConsumer Financial Protection Bureau's own motion, or upon the petition of any interested party.

[65 FR 40362, June 29, 2000, as amended at 89 FR 47786, June 3, 2024

§ 248.18 Effective date; transition rule.

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

(b)(1) *Notice requirement for consumers who are your customers on the compliance date.* By July 1, 2001, you must have provided an initial notice, as required by § 248.4, to consumers who are your customers on July 1, 2001.

(2) *Example.* You provide an initial notice to consumers who are your customers on July 1, 2001, if, by that date, you have established a system for providing an initial notice to all new customers and have mailed the initial notice to all your existing customers.

(c) *Two-year grandfathering of service agreements.* Until July 1, 2002, a contract that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 248.13(a)(2), even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as you entered into the agreement on or before July 1, 2000.

§§ 248.19–248.29 [Reserved]

§ 248.30 Procedures to safeguard customer information, including response programs for unauthorized access to customer information and customer notice; disposal of customer information and consumer information.

(a) *Policies and procedures to safeguard customer information*—(1) *General requirements.* Every covered institution must develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information.

(2) *Objectives.* These written policies and procedures must be reasonably designed to:

(i) Ensure the security and confidentiality of customer information;

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

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

(3) *Response programs for unauthorized access to or use of customer information.* Written policies and procedures in paragraph (a)(1) of this section must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:

(i) Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;

(ii) Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and

(iii) Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with paragraph (a)(4) of this section unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

(4) *Notifying affected individuals of unauthorized access or use*—(i) *Notification obligation.* Unless a covered institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information that occurred at the covered institution or one of its service providers that is not itself a covered institution, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience, the covered institution must provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.

(ii) *Affected individuals.* If an incident of unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, but the covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the covered institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization. Notwithstanding the foregoing, if the covered institution reasonably determines that a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization, the covered institution is not required to provide notice to that individual under this paragraph.

(iii) *Timing.* A covered institution must provide the notice as soon as practicable, but not later than 30 days,

after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred unless the United States Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, in which case the covered institution may delay providing such notice for a time period specified by the Attorney General, up to 30 days following the date when such notice was otherwise required to be provided. The notice may be delayed for an additional period of up to 30 days if the Attorney General determines that the notice continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, notice required under this section may be delayed for a final additional period of up to 60 days if the Attorney General determines that such notice continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph (a)(4)(iii), if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such delay through Commission exemptive order or other action.

(iv) *Notice contents.* The notice must:

(A) Describe in general terms the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization;

(B) Include, if the information is reasonably possible to determine at the time the notice is provided, any of the following: the date of the incident, the estimated date of the incident, or the date range within which the incident occurred;

(C) Include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including the following: a telephone number (which should be a toll-free number if available), an email address or equivalent method or means, a postal address, and the name of a specific office to contact for further information and assistance;

(D) If the individual has an account with the covered institution, recommend that the customer review account statements and immediately report any suspicious activity to the covered institution;

(E) Explain what a fraud alert is and how an individual may place a fraud alert in the individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft;

(F) Recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted;

(G) Explain how the individual may obtain a credit report free of charge; and

(H) Include information about the availability of online guidance from the Federal Trade Commission and *usa.gov* regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the Federal Trade Commission, and include the Federal Trade Commission's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.

(5) *Service providers.* (i) A covered institution's response program prepared in accordance with paragraph (a)(3) of this section must include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4) of this section. The policies and procedures must be reasonably designed to ensure service providers take appropriate measures to:

(A) Protect against unauthorized access to or use of customer information; and

(B) Provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming

aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider. Upon receipt of such notification, the covered institution must initiate its incident response program adopted pursuant to paragraph (a)(3) of this section.

(ii) As part of its incident response program, a covered institution may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf in accordance with paragraph (a)(4) of this section.

(iii) Notwithstanding a covered institution's use of a service provider in accordance with paragraphs (a)(5)(i) and (ii) of this section, the obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of this section rests with the covered institution.

(b) *Disposal of consumer information and customer information*—(1) *Standard.* Every covered institution, other than notice-registered broker-dealers, must properly dispose of consumer information and customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(2) *Written policies, procedures, and records.* Every covered institution, other than notice-registered broker-dealers, must adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information according to the standard identified in paragraph (b)(1) of this section.

(3) *Relation to other laws.* Nothing in this paragraph (b) shall be construed:

(i) To require any covered institution to maintain or destroy any record pertaining to an individual that is not imposed under other law; or

(ii) To alter or affect any requirement imposed under any other provision of law to maintain or destroy records.

(c) *Recordkeeping.* (1) Every covered institution that is an investment company under the Investment Company Act of 1940 (15 U.S.C. 80a), but is not registered under section 8 thereof (15 U.S.C. 80a–8), must make and maintain:

(i) The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(1) of this section;

(ii) The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by paragraph (a)(3) of this section;

(iii) The written documentation of any investigation and determination made regarding whether notification is required pursuant to paragraph (a)(4) of this section, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;

(iv) The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(5)(i) of this section;

(v) The written documentation of any contract or agreement entered into pursuant to paragraph (a)(5) of this section; and

(vi) The written policies and procedures required to be adopted and implemented pursuant to paragraph (b)(2) of this section.

(2) In the case of covered institutions described in paragraph (c)(1) of this section, such records, apart from any policies and procedures, must be preserved for a time period not less than six years, the first two years in an easily accessible place. In the case of policies and procedures required under paragraphs (a) and (b)(2) of this section, covered institutions described in paragraph (c)(1) of this section must maintain a copy of such policies and procedures in effect, or that at any time within the past six years were in effect, in an easily accessible place.

(d) *Definitions.* As used in this section, unless the context otherwise requires:

(1) *Consumer information* means:

(i) Any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report, or a

compilation of such records, that a covered institution maintains or otherwise possesses for a business purpose regardless of whether such information pertains to:

(A) Individuals with whom the covered institution has a customer relationship; or

(B) To the customers of other financial institutions where such information has been provided to the covered institution.

(ii) Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

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

(3) *Covered institution* means any broker or dealer, any investment company, and any investment adviser or transfer agent registered with the Commission or another appropriate regulatory agency (''ARA'') as defined in section 3(a)(34)(B) of the Securities Exchange Act of 1934.

(4) *Customer*. (i) Customer has the same meaning as in §248.3(j) unless the covered institution is a transfer agent registered with the Commission or another ARA.

(ii) With respect to a transfer agent registered with the Commission or another ARA, for purposes of this section, *customer* means any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent.

(5) *Customer information*. (i) Customer information for any covered institution other than a transfer agent registered with the Commission or another ARA means any record containing nonpublic personal information as defined in §248.3(t) about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf regardless of whether such information pertains to:

(A) Individuals with whom the covered institution has a customer relationship; or

(B) To the customers of other financial institutions where such information has been provided to the covered institution.

(ii) With respect to a transfer agent registered with the Commission or another ARA, *customer information* means any record containing nonpublic personal information as defined in §248.3(t) identified with any natural person, who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf, regardless of whether such information pertains to individuals with whom the transfer agent has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the transfer agent.

(6) *Customer information systems* means the information resources owned or used by a covered institution, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support the covered institution's operations.

(7) *Disposal* means:

(i) The discarding or abandonment of consumer information or customer information; or

(ii) The sale, donation, or transfer of any medium, including computer equipment, on which consumer information or customer information is stored.

(8) *Notice-registered broker-dealer* means a broker or dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)).

(9) *Sensitive customer information*. (i) Sensitive customer information means any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.

(ii) Examples of sensitive customer information include:

(A) Customer information uniquely identified with an individual that has a

reasonably likely use as a means of authenticating the individual's identity, including

(*1*) A Social Security number, official State- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(*2*) A biometric record;

(*3*) A unique electronic identification number, address, or routing code;

(*4*) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)); or

(B) Customer information identifying an individual or the individual's account, including the individual's account number, name or online user name, in combination with authenticating information such as information described in paragraph (d)(9)(ii)(A) of this section, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name.

(10) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

(11) *Transfer agent* has the same meaning as in section 3(a)(25) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).

[89 FR 47786, June 3, 2024]

§§ 248.31–248.100 [Reserved]

APPENDIX A TO SUBPART A OF PART 248—FORMS

A. Any person may view and print this form at: *http://www.sec.gov/about/forms/secforms.htm.*

B. Use of Form S–P by brokers, dealers, and investment companies, and investment advisers registered with the Commission constitutes compliance with the notice content requirements of §§ 248.6 and 248.7 of this part.

FORM S–P—MODEL PRIVACY FORM

A. The Model Privacy Form

Version 1: Model Form With No Opt-Out.

Rev. [insert date]

FACTS	WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [website]

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of financial institution] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of financial institution] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] **OR** [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

Version 2: Model Form with Opt-Out by Telephone and/or Online.

Rev. [insert date]

FACTS	WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call **[phone number]**—our menu will prompt you through your choice(s) **or** ■ Visit us online: **[website]** **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [website]

Page 2

Who we are	
Who is providing this notice?	[insert]

What we do	
How does [name of financial institution] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of financial institution] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] **OR** [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] **OR** [Your choices will apply to everyone on your account—unless you tell us otherwise.]

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*

Other important information
[insert other important information]

Version 3: Model Form with Mail-In Opt-Out Form.

Rev. [insert date]

FACTS	WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call **[phone number]**—our menu will prompt you through your choice(s) ■ Visit us online: **[website]** or ■ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [website]

✂

Mail-in Form

Leave Blank OR
[If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.
❑ Apply my choices only to me]

Mark any/all you want to limit:
❑ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.
❑ Do not allow your affiliates to use my personal information to market to me.
❑ Do not share my personal information with nonaffiliates to market their products and services to me.

Name
Address
City, State, Zip
[Account #]

Mail to:
[Name of Financial Institution]
[Address1]
[Address2]
[City], [ST] [ZIP]

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of financial institution] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of financial institution] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] **OR** [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] **OR** [Your choices will apply to everyone on your account—unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

Version 4. Optional Mail-in Form.

Mail-in Form		
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ❑ Apply my choices only to me]	Mark any/all you want to limit: ❑ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ❑ Do not allow your affiliates to use my personal information to market to me. ❑ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	

Mail To: [Name of Financial Institution], [Address1] [Address2], [City], [ST] [ZIP]

B. General Instructions

1. How the Model Privacy Form is Used

(a) The model form may be used, at the option of a financial institution, including a group of financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in §§248.6 and 248.7 of this part.

(b) The model form is a standardized form, including page layout, content, format, style, pagination, and shading. Institutions seeking to obtain the safe harbor through use of the model form may modify it only as described in these instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act [15 U.S.C. 1681–1681x] (FCRA), such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word ''customer'' may be replaced by the word ''member'' whenever it appears in the model form, as appropriate.

2. The Contents of the Model Privacy Form

The model form consists of two pages, which may be printed on both sides of a single sheet of paper, or may appear on two separate pages. Where an institution provides a long list of institutions at the end of the model form in accordance with Instruction C.3(a)(1), or provides additional information in accordance with Instruction C.3(c), and such list or additional information exceeds the space available on page two of the model form, such list or additional information may extend to a third page.

(a) *Page One*. The first page consists of the following components:

(1) Date last revised (upper right-hand corner).

(2) Title.

(3) Key frame (Why?, What?, How?).

(4) Disclosure table (''Reasons we can share your personal information'').

(5) ''To limit our sharing'' box, as needed, for the financial institution's opt-out information.

(6) ''Questions'' box, for customer service contact information.

(7) Mail-in opt-out form, as needed.

(b) *Page Two*. The second page consists of the following components:

(1) Heading (Page 2).

(2) Frequently Asked Questions (''Who we are'' and ''What we do'').

(3) Definitions.

(4) ''Other important information'' box, as needed.

3. The Format of the Model Privacy Form

The format of the model form may be modified only as described below.

(a) *Easily readable type font*. Financial institutions that use the model form must use an easily readable type font. While a number of factors together produce easily readable type font, institutions are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between the lines of type.

(b) *Logo*. A financial institution may include a corporate logo on any page of the notice, so long as it does not interfere with the

readability of the model form or the space constraints of each page.

(c) *Page size and orientation.* Each page of the model form must be printed on paper in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) *Color.* The model form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the model form. Logos may also be printed in color.

(e) *Languages.* The model form may be translated into languages other than English.

C. Information Required in the Model Privacy Form

The information in the model form may be modified only as described below:

1. Name of the Institution or Group of Affiliated Institutions Providing the Notice

Insert the name of the financial institution providing the notice or a common identity of affiliated institutions jointly providing the notice on the form wherever [name of financial institution] appears.

2. Page One

(a) *Last revised date.* The financial institution must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as ''rev. [month/year]'' using either the name or number of the month, such as ''rev. July 2009'' or ''rev. 7/09''.

(b) *General instructions for the ''What?'' box.* (1) The bulleted list identifies the types of personal information that the institution collects and shares. All institutions must use the term ''Social Security number'' in the first bullet.

(2) Institutions must use five (5) of the following terms to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) *General instructions for the disclosure table.* The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in paragraph C.2(d) of this Instruction. In the middle column, each institution must provide a ''Yes'' or ''No'' response that accurately reflects its information sharing policies and practices with respect to the reason listed on the left. In the right column, each institution must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing: ''Yes'' if it is required to or voluntarily provides an opt-out; ''No'' if it does not provide an opt-out; or ''We don't share'' if it answers ''No'' in the middle column. Only the sixth row (''For our affiliates to market to you'') may be omitted at the option of the institution. *See* paragraph C.2(d)(6) of this Instruction.

(d) *Specific disclosures and corresponding legal provisions.* (1) *For our everyday business purposes.* This reason incorporates sharing information under §§248.14 and 248.15 and with service providers pursuant to §248.13 of this part other than the purposes specified in paragraphs C.2(d)(2) or C.2(d)(3) of these Instructions.

(2) *For our marketing purposes.* This reason incorporates sharing information with service providers by an institution for its own marketing pursuant to §248.13 of this part. An institution that shares for this reason may choose to provide an opt-out.

(3) *For joint marketing with other financial companies.* This reason incorporates sharing information under joint marketing agreements between two or more financial institutions and with any service provider used in connection with such agreements pursuant to §248.13 of this part. An institution that shares for this reason may choose to provide an opt-out.

(4) *For our affiliates' everyday business purposes—information about transactions and experiences.* This reason incorporates sharing information specified in sections 603(d)(2)(A)(i) and (ii) of the FCRA. An institution that shares for this reason may choose to provide an opt-out.

(5) *For our affiliates' everyday business purposes—information about creditworthiness.* This reason incorporates sharing information pursuant to section 603(d)(2)(A)(iii) of the FCRA. An institution that shares for this reason must provide an opt-out.

(6) *For our affiliates to market to you.* This reason incorporates sharing information specified in section 624 of the FCRA. This reason may be omitted from the disclosure table when: the institution does not have affiliates (or does not disclose personal information to its affiliates); the institution's affiliates do not use personal information in a manner that requires an opt-out; or the institution provides the affiliate marketing notice separately. Institutions that include

this reason must provide an opt-out of indefinite duration. An institution that is required to provide an affiliate marketing opt-out, but does not include that opt-out in the model form under this part, must comply with section 624 of the FCRA and 17 CFR part 248, subpart B, with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. An institution not required to provide an opt-out under this subparagraph may elect to include this reason in the model form.

(7) *For nonaffiliates to market to you.* This reason incorporates sharing described in §§248.7 and 248.10(a) of this part. An institution that shares personal information for this reason must provide an opt-out.

(e) *To limit our sharing:* A financial institution must include this section of the model form *only* if it provides an opt-out. The word ''choice'' may be written in either the singular or plural, as appropriate. Institutions must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a Web site; or use of a mail-in opt-out form. Institutions may include the words ''toll-free'' before telephone, as appropriate. An institution that allows consumers to opt out online must provide either a specific Web address that takes consumers directly to the opt-out page or a general Web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the institution through these methods must correspond accurately to the ''Yes'' responses in the third column of the disclosure table. In the part titled ''Please note'' institutions may insert a number that is 30 or greater in the space marked ''[30].'' Instructions on voluntary or state privacy law opt-out information are in paragraph C.2(g)(5) of these Instructions.

(f) *Questions box.* Customer service contact information must be inserted as appropriate, where [phone number] or [Web site] appear. Institutions may elect to provide either a phone number, such as a toll-free number, or a Web address, or both. Institutions may include the words ''toll-free'' before the telephone number, as appropriate.

(g) *Mail-in opt-out form.* Financial institutions must include this mail-in form *only* if they state in the ''To limit our sharing'' box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the ''Yes'' responses in the third column in the disclosure table. Institutions that require customers to provide only name and address may omit the section identified as ''[account #].'' Institutions that require additional or different information, such as a random opt-out number or a truncated account number, to implement an opt-out election should modify the ''[account #]'' reference accordingly. This includes institutions that require customers with multiple accounts to identify each account to which the opt-out should apply. An institution must enter its opt-out mailing address: in the far right of this form (*see* version 3); or below the form (*see* version 4). The reverse side of the mail-in opt-out form must not include any content of the model form.

(1) *Joint accountholder.* Only institutions that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with paragraph C.3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement: ''If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choice(s) only to me.'' The word ''choice'' may be written in either the singular or plural, as appropriate. Financial institutions that provide insurance products or services, provide this option, and elect to use the model form may substitute the word ''policy'' for ''account'' in this statement. Institutions that do not provide this option may eliminate this left column from the mail-in form.

(2) *FCRA Section 603(d)(2)(A)(iii) opt-out.* If the institution shares personal information pursuant to section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement: ''☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.''

(3) *FCRA Section 624 opt-out.* If the institution incorporates section 624 of the FCRA in accord with paragraph C.2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement: ''☐ Do not allow your affiliates to use my personal information to market to me.''

(4) *Nonaffiliate opt-out.* If the financial institution shares personal information pursuant to §248.10(a) of this part, it must include in the mail-in opt-out form the following statement: ''☐ Do not share my personal information with nonaffiliates to market their products and services to me.''

(5) *Additional opt-outs.* Financial institutions that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the model form. A financial institution that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements: ''☐ Do not share my personal information to market to me.'' *or* ''☐ Do not use my personal information to market to me.'' A financial institution that chooses to offer an opt-out for joint marketing must include the following statement: ''☐ Do not share my personal information with other financial institutions to jointly market to me.''

(h) *Barcodes.* A financial institution may elect to include a barcode and/or ''tagline'' (an internal identifier) in 6-point font at the bottom of page one, as needed for information internal to the institution, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) *General Instructions for the Questions.* Certain of the Questions may be customized as follows:

(1) ''*Who is providing this notice?*'' This question may be omitted where only one financial institution provides the model form and that institution is clearly identified in the title on page one. Two or more financial institutions that jointly provide the model form must use this question to identify themselves as required by §248.9(f) of this part. Where the list of institutions exceeds four (4) lines, the institution must describe in the response to this question the general types of institutions jointly providing the notice and must separately identify those institutions, in minimum 8-point font, directly following the ''Other important information'' box, or, if that box is not included in the institution's form, directly following the ''Definitions.'' The list may appear in a multi-column format.

(2) ''*How does [name of financial institution] protect my personal information?*'' The financial institution may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the institution's use of cookies or other measures it uses to safeguard personal information. Institutions are limited to a maximum of 30 additional words.

(3) ''*How does [name of financial institution] collect my personal information?*'' Institutions must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade. Institutions that collect personal information from their affiliates and/or credit bureaus must include after the bulleted list the following statement: ''We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.'' Institutions that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: ''We also collect your personal information from other companies.'' Only institutions that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(4) ''*Why can't I limit all sharing?*'' Institutions that describe state privacy law provisions in the ''*Other important information*'' box must use the bracketed sentence: ''See below for more on your rights under state law.'' Other institutions must omit this sentence.

(5) ''*What happens when I limit sharing for an account I hold jointly with someone else?*'' Only financial institutions that provide opt-out options must use this question. Other institutions must omit this question. Institutions must choose one of the following two statements to respond to this question: ''Your choices will apply to everyone on your account.'' or ''Your choices will apply to everyone on your account—unless you tell us otherwise.'' Financial institutions that provide insurance products or services and elect to use the model form may substitute the word ''policy'' for ''account'' in these statements.

(b) *General Instructions for the Definitions.* The financial institution must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(1) *Affiliates.* As required by §248.6(a)(3) of this part, where [*affiliate information*] appears, the financial institution must:

(i) If it has no affiliates, state: ''[*name of financial institution*] has no affiliates;''

(ii) If it has affiliates but does not share personal information, state: ''[*name of financial institution*] does not share with our affiliates;'' or

(iii) If it shares with its affiliates, state, as applicable: ''Our affiliates include companies with a [*common corporate identity of financial institution*] name; financial companies such as [*insert illustrative list of companies*]; nonfinancial companies, such as [*insert illustrative list of companies*] and others, such as [*insert illustrative list*].''

(2) *Nonaffiliates.* As required by §248.6(c)(3) of this part, where [*nonaffiliate information*] appears, the financial institution must:

(i) If it does not share with nonaffiliated third parties, state: ''[*name of financial institution*] does not share with nonaffiliates so they can market to you;'' or

(ii) If it shares with nonaffiliated third parties, state, as applicable: ''Nonaffiliates we share with can include [*list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations*].''

(3) *Joint Marketing.* As required by §248.13 of this part, where [*joint marketing*] appears, the financial institution must:

(i) If it does not engage in joint marketing, state: ''[*name of financial institution*] doesn't jointly market;'' or

(ii) If it shares personal information for joint marketing, state, as applicable: ''Our joint marketing partners include [*list categories of companies such as credit card companies*].''

(c) *General instructions for the ''Other important information'' box.* This box is optional. The space provided for information in this box is not limited. Only the following types of information can appear in this box.

(1) State and/or international privacy law information; and/or

(2) Acknowledgment of receipt form.

[74 FR 62985, Dec. 1, 2009]

Subpart B—Regulation S-AM: Limitations on Affiliate Marketing

SOURCE: 74 FR 40431, Aug. 11, 2009, unless otherwise noted.

§ 248.101 Purpose and scope.

(a) *Purpose.* The purpose of this subpart is to implement section 624 of the Fair Credit Reporting Act, 15 U.S.C. 1681, *et seq.* (''FCRA''). Section 624, which was added to the FCRA by section 214 of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108–159, 117 Stat. 1952 (2003) (''FACT Act'' or ''Act''), regulates the use of consumer information received from an affiliate to make marketing solicitations.

(b) *Scope.* This subpart applies to any broker or dealer other than a notice-registered broker or dealer, to any investment company, and to any investment adviser or transfer agent registered with the Commission. These entities are referred to in this subpart as ''you.''

§ 248.102 Examples.

The examples in this subpart are not exclusive. The examples in this subpart provide guidance concerning the rules' application in ordinary circumstances. The facts and circumstances of each individual situation, however, will determine whether compliance with an example, to the extent applicable, constitutes compliance with this subpart. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise under this subpart. Similarly, the examples do not illustrate any issues that may arise under other laws or regulations.

§§ 248.103–248.119 [Reserved]

§ 248.120 Definitions.

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

(a) *Affiliate* of a broker, dealer, or investment company, or an investment adviser or transfer agent registered with the Commission means any person that is related by common ownership or common control with the broker, dealer, or investment company, or the investment adviser or transfer agent registered with the Commission. In addition, a broker, dealer, or investment company, or an investment adviser or transfer agent registered with the Commission will be deemed an affiliate of a company for purposes of this subpart if:

(1) That company is regulated under section 214 of the FACT Act, Public Law 108–159, 117 Stat. 1952 (2003), by a government regulator other than the Commission; and

(2) Rules adopted by the other government regulator under section 214 of the FACT Act treat the broker, dealer, or investment company, or investment adviser or transfer agent 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)). A ''broker'' does not include a broker registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)).

(c) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

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

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

(f) *Concise*—(1) *In general.* The term ''concise'' means a reasonably brief expression or statement.

(2) *Combination with other required disclosures.* A notice required by this subpart may be concise even if it is combined with other disclosures required or authorized by Federal or State law.

(g) *Consumer* means an individual.

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

(i) *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)). A ''dealer'' does not include a dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)).

(j) *Eligibility information* means any information the communication of which would be a consumer report if the exclusions from the definition of ''consumer report'' in section 603(d)(2)(A) of the FCRA did not apply. Eligibility information does not include aggregate or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(k) *FCRA* means the Fair Credit Reporting Act (15 U.S.C. 1681, *et seq.*).

(l) *GLBA* means the Gramm-Leach-Bliley Act (15 U.S.C. 6801, *et seq.*).

(m) *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)).

(n) *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.

(o) *Marketing solicitation*—(1) *In general.* The term ''marketing solicitation'' means the marketing of a product or service initiated by a person to a particular consumer that is:

(i) Based on eligibility information communicated to that person by its affiliate as described in this subpart; and

(ii) Intended to encourage the consumer to purchase or obtain such product or service.

(2) *Exclusion of marketing directed at the general public.* A marketing solicitation does not include marketing communications that are directed at the general public. For example, television, general circulation magazine, billboard advertisements and publicly available Web sites that are not directed to particular consumers would not constitute marketing solicitations, even if those communications are intended to encourage consumers to purchase products and services from the person initiating the communications.

(3) *Examples of marketing solicitations.* A marketing solicitation would include, for example, a telemarketing call, direct mail, e-mail, or other form of marketing communication directed to a particular consumer that is based on eligibility information received from an affiliate.

(p) *Person* means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

(q) *Pre-existing business relationship*—(1) *In general.* The term ''pre-existing business relationship'' means a relationship between a person, or a person's licensed agent, and a consumer based on:

(i) A financial contract between the person and the consumer which is in force on the date on which the consumer is sent a solicitation covered by this subpart;

(ii) The purchase, rental, or lease by the consumer of the person's goods or services, or a financial transaction (including holding an active account or a policy in force or having another continuing relationship) between the consumer and the person, during the 18-month period immediately preceding the date on which the consumer is sent a solicitation covered by this subpart; or

(iii) An inquiry or application by the consumer regarding a product or service offered by that person during the three-month period immediately preceding the date on which the consumer is sent a solicitation covered by this subpart.

(2) *Examples of pre-existing business relationships.* (i) If a consumer has a brokerage account with a broker-dealer that is currently in force, the broker-dealer has a pre-existing business relationship with the consumer and can use eligibility information it receives from its affiliates to make solicitations to the consumer about its products or services.

(ii) If a consumer has an investment advisory contract with a registered investment adviser, the investment adviser has a pre-existing business relationship with the consumer and can use eligibility information it receives from its affiliates to make solicitations to the consumer about its products or services.

(iii) If a consumer was the record owner of securities issued by an investment company, but the consumer redeems these securities, the investment company has a pre-existing business relationship with the consumer and can use eligibility information it receives from its affiliates to make solicitations to the consumer about its products or services for 18 months after the date the consumer redeemed the investment company's securities.

(iv) If a consumer applies for a margin account offered by a broker-dealer, but does not obtain a product or service from or enter into a financial contract or transaction with the broker-dealer, the broker-dealer has a pre-existing business relationship with the consumer and can therefore use eligibility information it receives from its affiliates to make solicitations to the consumer about its products or services for three months after the date of the application.

(v) If a consumer makes a telephone inquiry to a broker-dealer about its products or services and provides contact information to the broker-dealer, but does not obtain a product or service from or enter into a financial contract or transaction with the institution, the broker-dealer has a pre-existing business relationship with the consumer and can therefore use eligibility information it receives from its affiliates to make solicitations to the consumer about its products or services for three months after the date of the inquiry.

(vi) If a consumer makes an inquiry by e-mail to a broker-dealer about one of its affiliated investment company's products or services but does not obtain a product or service from, or enter into a financial contract or transaction with the broker-dealer or the investment company, the broker-dealer and the investment company both have a pre-existing business relationship with the consumer and can therefore use eligibility information they receive from their affiliates to make solicitations to the consumer about their products or services for three months after the date of the inquiry.

(vii) If a consumer who has a pre-existing business relationship with an investment company that is part of a group of affiliated companies makes a telephone call to the centralized call center for the affiliated companies to inquire about products or services offered by a broker-dealer affiliated with the investment company, and provides contact information to the call center, the call constitutes an inquiry to the broker-dealer. In these circumstances, the broker-dealer has a pre-existing business relationship with the consumer and can therefore use eligibility information it receives from the investment company to make solicitations to the consumer about its products or services for three months after the date of the inquiry.

(3) *Examples where no pre-existing business relationship is created.* (i) If a consumer makes a telephone call to a centralized call center for a group of affiliated companies to inquire about the

consumer's existing account at a broker-dealer, the call does not constitute an inquiry to any affiliate other than the broker-dealer that holds the consumer's account and does not establish a pre-existing business relationship between the consumer and any affiliate of the account-holding broker-dealer.

(ii) If a consumer who has an advisory contract with a registered investment adviser makes a telephone call to an affiliate of the investment adviser to ask about the affiliate's retail locations and hours, but does not make an inquiry about the affiliate's products or services, the call does not constitute an inquiry and does not establish a pre-existing business relationship between the consumer and the affiliate. Also, the affiliate's capture of the consumer's telephone number does not constitute an inquiry and does not establish a pre-existing business relationship between the consumer and the affiliate.

(iii) If a consumer makes a telephone call to a broker-dealer in response to an advertisement offering a free promotional item to consumers who call a toll-free number, but the advertisement does not indicate that the broker-dealer's products or services will be marketed to consumers who call in response, the call does not create a pre-existing business relationship between the consumer and the broker-dealer because the consumer has not made an inquiry about a product or service offered by the institution, but has merely responded to an offer for a free promotional item.

(r) *Transfer agent* has the same meaning as in section 3(a)(25) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).

(s) *You* means:

(1) Any broker or dealer other than a broker or dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11));

(2) Any investment company;

(3) Any investment adviser registered with the Commission under the Investment Advisers Act of 1940 (15 U.S.C. 80b–1, *et seq.*); and

(4) Any transfer agent registered with the Commission under section 17A of the Securities Exchange Act of 1934 (15 U.S.C. 78q–1).

§ 248.121 Affiliate marketing opt out and exceptions.

(a) *Initial notice and opt out requirement*—(1) *In general.* You may not use eligibility information about a consumer that you receive from an affiliate to make a marketing solicitation to the consumer, unless:

(i) It is clearly and conspicuously disclosed to the consumer in writing or, if the consumer agrees, electronically, in a concise notice that you may use eligibility information about that consumer received from an affiliate to make marketing solicitations to the consumer;

(ii) The consumer is provided a reasonable opportunity and a reasonable and simple method to ''opt out,'' or the consumer prohibits you from using eligibility information to make marketing solicitations to the consumer; and

(iii) The consumer has not opted out.

(2) *Example.* A consumer has a brokerage account with a broker-dealer. The broker-dealer furnishes eligibility information about the consumer to its affiliated investment adviser. Based on that eligibility information, the investment adviser wants to make a marketing solicitation to the consumer about its discretionary advisory accounts. The investment adviser does not have a pre-existing business relationship with the consumer and none of the other exceptions apply. The investment adviser is prohibited from using eligibility information received from its broker-dealer affiliate to make marketing solicitations to the consumer about its discretionary advisory accounts unless the consumer is given a notice and opportunity to opt out and the consumer does not opt out.

(3) *Affiliates who may provide the notice.* The notice required by this paragraph must be provided:

(i) By an affiliate that has or has previously had a pre-existing business relationship with the consumer; or

(ii) As part of a joint notice from two or more members of an affiliated group of companies, provided that at least one of the affiliates on the joint notice

has or has previously had a pre-existing business relationship with the consumer.

(b) *Making marketing solicitations*—(1) *In general.* For purposes of this subpart, you make a marketing solicitation if:

(i) You receive eligibility information from an affiliate;

(ii) You use that eligibility information to do one or more of the following:

(A) Identify the consumer or type of consumer to receive a marketing solicitation;

(B) Establish criteria used to select the consumer to receive a marketing solicitation; or

(C) Decide which of your products or services to market to the consumer or tailor your marketing solicitation to that consumer; and

(iii) As a result of your use of the eligibility information, the consumer is provided a marketing solicitation.

(2) *Receiving eligibility information from an affiliate, including through a common database.* You may receive eligibility information from an affiliate in various ways, including when the affiliate places that information into a common database that you may access.

(3) *Receipt or use of eligibility information by your service provider.* Except as provided in paragraph (b)(5) of this section, you receive or use an affiliate's eligibility information if a service provider acting on your behalf (whether an affiliate or a nonaffiliated third party) receives or uses that information in the manner described in paragraph (b)(1)(i) or (b)(1)(ii) of this section. All relevant facts and circumstances will determine whether a person is acting as your service provider when it receives or uses an affiliate's eligibility information in connection with marketing your products and services.

(4) *Use by an affiliate of its own eligibility information.* Unless you have used eligibility information that you receive from an affiliate in the manner described in paragraph (b)(1)(ii) of this section, you do not make a marketing solicitation subject to this subpart if your affiliate:

(i) Uses its own eligibility information that it obtained in connection with a pre-existing business relationship it has or had with the consumer to market your products or services to the affiliate's consumer; or

(ii) Directs its service provider to use the affiliate's own eligibility information that it obtained in connection with a pre-existing business relationship it has or had with the consumer to market your products or services to the consumer, and you do not communicate directly with the service provider regarding that use.

(5) *Use of eligibility information by a service provider*—(i) *In general.* You do not make a marketing solicitation subject to this subpart if a service provider (including an affiliated or third-party service provider that maintains or accesses a common database that you may access) receives eligibility information from your affiliate that your affiliate obtained in connection with a pre-existing business relationship it has or had with the consumer and uses that eligibility information to market your products or services to that affiliate's consumer, so long as:

(A) Your affiliate controls access to and use of its eligibility information by the service provider (including the right to establish the specific terms and conditions under which the service provider may use such information to market your products or services);

(B) Your affiliate establishes specific terms and conditions under which the service provider may access and use your affiliate's eligibility information to market your products and services (or those of affiliates generally) to your affiliate's consumers, such as the identity of the affiliated companies whose products or services may be marketed to the affiliate's consumers by the service provider, the types of products or services of affiliated companies that may be marketed, and the number of times your affiliate's consumers may receive marketing materials, and periodically evaluates the service provider's compliance with those terms and conditions;

(C) Your affiliate requires the service provider to implement reasonable policies and procedures designed to ensure that the service provider uses your affiliate's eligibility information in accordance with the terms and conditions established by your affiliate relating to

the marketing of your products or services;

(D) Your affiliate is identified on or with the marketing materials provided to the consumer; and

(E) You do not directly use your affiliate's eligibility information in the manner described in paragraph (b)(1)(ii) of this section.

(ii) *Writing requirements.* (A) The requirements of paragraphs (b)(5)(i)(A) and (C) of this section must be set forth in a written agreement between your affiliate and the service provider; and

(B) The specific terms and conditions established by your affiliate as provided in paragraph (b)(5)(i)(B) of this section must be set forth in writing.

(6) *Examples of making marketing solicitations.* (i) A consumer has an investment advisory contract with a registered investment adviser that is affiliated with a broker-dealer. The broker-dealer receives eligibility information about the consumer from the investment adviser. The broker-dealer uses that eligibility information to identify the consumer to receive a marketing solicitation about brokerage products and services, and, as a result, the broker-dealer provides a marketing solicitation to the consumer about its brokerage services. Pursuant to paragraph (b)(1) of this section, the broker-dealer has made a marketing solicitation to the consumer.

(ii) The same facts as in the example in paragraph (b)(6)(i) of this section, except that after using the eligibility information to identify the consumer to receive a marketing solicitation about brokerage products and services, the broker-dealer asks the registered investment adviser to send the marketing solicitation to the consumer and the investment adviser does so. Pursuant to paragraph (b)(1) of this section, the broker-dealer has made a marketing solicitation to the consumer because it used eligibility information about the consumer that it received from an affiliate to identify the consumer to receive a marketing solicitation about its products or services, and, as a result, a marketing solicitation was provided to the consumer about the broker-dealer's products and services.

(iii) The same facts as in the example in paragraph (b)(6)(i) of this section, except that eligibility information about consumers who have an investment advisory contract with a registered investment adviser is placed into a common database that all members of the affiliated group of companies may independently access and use. Without using the investment adviser's eligibility information, the broker-dealer develops selection criteria and provides those criteria, marketing materials, and related instructions to the investment adviser. The investment adviser reviews eligibility information about its own consumers using the selection criteria provided by the broker-dealer to determine which consumers should receive the broker-dealer's marketing materials and sends the broker-dealer's marketing materials to those consumers. Even though the broker-dealer has received eligibility information through the common database as provided in paragraph (b)(2) of this section, it did not use that information to identify consumers or establish selection criteria; instead, the investment adviser used its own eligibility information. Therefore, pursuant to paragraph (b)(4)(i) of this section, the broker-dealer has not made a marketing solicitation to the consumer.

(iv) The same facts as in the example in paragraph (b)(6)(iii) of this section, except that the registered investment adviser provides the broker-dealer's criteria to the investment adviser's service provider and directs the service provider to use the investment adviser's eligibility information to identify investment adviser consumers who meet the criteria and to send the broker-dealer's marketing materials to those consumers. The broker-dealer does not communicate directly with the service provider regarding the use of the investment adviser's information to market its products or services to the investment adviser's consumers. Pursuant to paragraph (b)(4)(ii) of this section, the broker-dealer has not made a marketing solicitation to the consumer.

(v) An affiliated group of companies includes an investment company, a principal underwriter for the investment company, a retail broker-dealer,

and a transfer agent that also acts as a service provider. Each affiliate in the group places information about its consumers into a common database. The service provider has access to all information in the common database. The investment company controls access to and use of its eligibility information by the service provider. This control is set forth in a written agreement between the investment company and the service provider. The written agreement also requires the service provider to establish reasonable policies and procedures designed to ensure that the service provider uses the investment company's eligibility information in accordance with specific terms and conditions established by the investment company relating to the marketing of the products and services of all affiliates, including the principal underwriter and the retail broker-dealer. In a separate written communication, the investment company specifies the terms and conditions under which the service provider may use the investment company's eligibility information to market the retail broker-dealer's products and services to the investment company's consumers. The specific terms and conditions are: a list of affiliated companies (including the retail broker-dealer) whose products or services may be marketed to the investment company's consumers by the service provider; the specific products or services or types of products or services that may be marketed to the investment company's consumers by the service provider; the categories of eligibility information that may be used by the service provider in marketing products or services to the investment company's consumers; the types or categories of the investment company's consumers to whom the service provider may market products or services of investment company affiliates; the number and types of marketing communications that the service provider may send to the investment company's consumers; and the length of time during which the service provider may market the products or services of the investment company's affiliates to its consumers. The investment company periodically evaluates the service provider's compliance with these terms and conditions. The retail broker-dealer asks the service provider to market brokerage services to certain of the investment company's consumers. Without using the investment company's eligibility information, the retail broker-dealer develops selection criteria and provides those criteria, its marketing materials, and related instructions to the service provider. The service provider uses the investment company's eligibility information from the common database to identify the investment company's consumers to whom brokerage services will be marketed. When the retail broker-dealer's marketing materials are provided to the identified consumers, the name of the investment company is displayed on the retail broker-dealer's marketing materials, an introductory letter that accompanies the marketing materials, an account statement that accompanies the marketing materials, or the envelope containing the marketing materials. The requirements of paragraph (b)(5) of this section have been satisfied, and the retail broker-dealer has not made a marketing solicitation to the consumer.

(vi) The same facts as in the example in paragraph (b)(6)(v) of this section, except that the terms and conditions permit the service provider to use the investment company's eligibility information to market the products and services of other affiliates to the investment company's consumers whenever the service provider deems it appropriate to do so. The service provider uses the investment company's eligibility information in accordance with the discretion afforded to it by the terms and conditions. Because the terms and conditions are not specific, the requirements of paragraph (b)(5) of this section have not been satisfied.

(c) *Exceptions.* The provisions of this subpart do not apply to you if you use eligibility information that you receive from an affiliate:

(1) To make a marketing solicitation to a consumer with whom you have a pre-existing business relationship;

(2) To facilitate communications to an individual for whose benefit you provide employee benefit or other services pursuant to a contract with an employer related to and arising out of the

current employment relationship or status of the individual as a participant or beneficiary of an employee benefit plan;

(3) To perform services on behalf of an affiliate, except that this paragraph shall not be construed as permitting you to send marketing solicitations on behalf of an affiliate if the affiliate would not be permitted to send the marketing solicitation as a result of the election of the consumer to opt out under this subpart;

(4) In response to a communication about your products or services initiated by the consumer;

(5) In response to an authorization or request by the consumer to receive solicitations; or

(6) If your compliance with this subpart would prevent you from complying with any provision of State insurance laws pertaining to unfair discrimination in any State in which you are lawfully doing business.

(d) *Examples of exceptions*—(1) *Example of the pre-existing business relationship exception.* A consumer has a brokerage account with a broker-dealer. The consumer also has a deposit account with the broker-dealer's affiliated depository institution. The broker-dealer receives eligibility information about the consumer from its depository institution affiliate and uses that information to make a marketing solicitation to the consumer about the broker-dealer's college savings accounts. The broker-dealer may make this marketing solicitation even if the consumer has not been given a notice and opportunity to opt out because the broker-dealer has a pre-existing business relationship with the consumer.

(2) *Examples of service provider exception.* (i) A consumer has a brokerage account with a broker-dealer. The broker-dealer furnishes eligibility information about the consumer to its affiliate, a registered investment adviser. Based on that eligibility information, the investment adviser wants to make a marketing solicitation to the consumer about its advisory services. The investment adviser does not have a pre-existing business relationship with the consumer and none of the other exceptions in paragraph (c) of this section apply. The consumer has been given an opt out notice and has elected to opt out of receiving such marketing solicitations. The investment adviser asks a service provider to send the marketing solicitation to the consumer on its behalf. The service provider may not send the marketing solicitation on behalf of the investment adviser because, as a result of the consumer's opt out election, the investment adviser is not permitted to make the marketing solicitation.

(ii) The same facts as in paragraph (d)(2)(i) of this section, except the consumer has been given an opt out notice, but has not elected to opt out. The investment adviser asks a service provider to send the solicitation to the consumer on its behalf. The service provider may send the marketing solicitation on behalf of the investment adviser because, as a result of the consumer's not opting out, the investment adviser is permitted to make the marketing solicitation.

(3) *Examples of consumer-initiated communications.* (i) A consumer who is the record owner of shares in an investment company initiates a communication with an affiliated registered investment adviser about advisory services. The affiliated investment adviser may use eligibility information about the consumer it obtains from the investment company or any other affiliate to make marketing solicitations regarding the affiliated investment adviser's services in response to the consumer-initiated communication.

(ii) A consumer who has a brokerage account with a broker-dealer contacts the broker-dealer to request information about how to save and invest for a child's college education without specifying the type of savings or investment vehicle in which the consumer may be interested. Information about a range of different products or services offered by the broker-dealer and one or more of its affiliates may be responsive to that communication. Such products, services, and investments may include the following: investments in affiliated investment companies; investments in section 529 plans offered by the broker-dealer; or trust services offered by a different financial institution in the affiliated group. Any affiliate offering

products or services that would be responsive to the consumer's request for information about saving and investing for a child's college education may use eligibility information to make marketing solicitations to the consumer in response to this communication.

(iii) A registered investment adviser makes a marketing call to the consumer without using eligibility information received from an affiliate. The investment adviser leaves a voice-mail message that invites the consumer to call a toll-free number to receive information about services offered by the investment adviser. If the consumer calls the toll-free number to inquire about the investment advisory services, the call is a consumer-initiated communication about a product or service, and the investment adviser may now use eligibility information it receives from its affiliates to make marketing solicitations to the consumer.

(iv) A consumer calls a broker-dealer to ask about retail locations and hours, but does not request information about its products or services. The broker-dealer may not use eligibility information it receives from an affiliate to make marketing solicitations to the consumer because the consumer-initiated communication does not relate to the broker-dealer's products or services. Thus, the use of eligibility information received from an affiliate would not be responsive to the communication and the exception does not apply.

(v) A consumer calls a broker-dealer to ask about retail locations and hours. The customer service representative asks the consumer if there is a particular product or service about which the consumer is seeking information. The consumer responds that the consumer wants to stop in and find out about mutual funds (i.e., registered open-end investment companies). The customer service representative offers to provide that information by telephone and mail additional information to the consumer. The consumer agrees and provides or confirms contact information for receipt of the materials to be mailed. The broker-dealer may use eligibility information it receives from an affiliate to make marketing solicitations to the consumer about mutual funds because such marketing solicitations would respond to the consumer-initiated communication about mutual funds.

(4) *Examples of consumer authorization or request for marketing solicitations.* (i) A consumer who has a brokerage account with a broker-dealer authorizes or requests information about life insurance offered by the broker-dealer's insurance affiliate. The authorization or request, whether given to the broker-dealer or the insurance affiliate, would permit the insurance affiliate to use eligibility information about the consumer it obtains from the broker-dealer or any other affiliate to make marketing solicitations to the consumer about life insurance.

(ii) A consumer completes an online application to open an online brokerage account with a broker-dealer. The broker-dealer's online application contains a blank check box that the consumer may check to authorize or request information from the broker-dealer's affiliates. The consumer checks the box. The consumer has authorized or requested marketing solicitations from the broker-dealer's affiliates.

(iii) A consumer completes an online application to open an online brokerage account with a broker-dealer. The broker-dealer's online application contains a check box indicating that the consumer authorizes or requests information from the broker-dealer's affiliates. The consumer does not deselect the check box. The consumer has not authorized or requested marketing solicitations from the broker-dealer's affiliates.

(iv) The terms and conditions of a brokerage account agreement contain preprinted boilerplate language stating that by applying to open an account the consumer authorizes or requests to receive solicitations from the broker-dealer's affiliates. The consumer has not authorized or requested marketing solicitations from the broker-dealer's affiliates.

(e) *Relation to affiliate-sharing notice and opt out.* Nothing in this subpart limits the responsibility of a person to comply with the notice and opt out provisions of Section 603(d)(2)(A)(iii) of

the FCRA (15 U.S.C. 1681a(d)(2)(A)(iii)) where applicable.

§ 248.122 Scope and duration of opt out.

(a) *Scope of opt out*—(1) *In general.* Except as otherwise provided in this section, the consumer's election to opt out prohibits any affiliate covered by the opt out notice from using eligibility information received from another affiliate as described in the notice to make marketing solicitations to the consumer.

(2) *Continuing relationship*—(i) *In general.* If the consumer establishes a continuing relationship with you or your affiliate, an opt out notice may apply to eligibility information obtained in connection with:

(A) A single continuing relationship or multiple continuing relationships that the consumer establishes with you or your affiliates, including continuing relationships established subsequent to delivery of the opt out notice, so long as the notice adequately describes the continuing relationships covered by the opt out; or

(B) Any other transaction between the consumer and you or your affiliates as described in the notice.

(ii) *Examples of continuing relationships.* A consumer has a continuing relationship with you or your affiliate if the consumer:

(A) Opens a brokerage account or enters into an advisory contract with you or your affiliate;

(B) Obtains a loan for which you or your affiliate owns the servicing rights;

(C) Purchases investment company shares in his or her own name;

(D) Holds an investment through you or your affiliate; such as when you act or your affiliate acts as a custodian for securities or for assets in an individual retirement arrangement;

(E) Enters into an agreement or understanding with you or your affiliate whereby you or your affiliate undertakes to arrange or broker a home mortgage loan for the consumer;

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

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

(3) *No continuing relationship*—(i) *In general.* If there is no continuing relationship between a consumer and you or your affiliate, and you or your affiliate obtain eligibility information about a consumer in connection with a transaction with the consumer, such as an isolated transaction or an application that is denied, an opt out notice provided to the consumer only applies to eligibility information obtained in connection with that transaction.

(ii) *Examples of isolated transactions.* An isolated transaction occurs if:

(A) The consumer uses your or your affiliate's ATM to withdraw cash from an account at another financial institution; or

(B) A broker-dealer opens a brokerage account for the consumer solely for the purpose of liquidating or purchasing securities as an accommodation, i.e., on a one-time basis, without the expectation of engaging in other transactions.

(4) *Menu of alternatives.* A consumer may be given the opportunity to choose from a menu of alternatives when electing to prohibit solicitations, such as by electing to prohibit solicitations from certain types of affiliates covered by the opt out notice but not other types of affiliates covered by the notice, electing to prohibit marketing solicitations based on certain types of eligibility information but not other types of eligibility information, or electing to prohibit marketing solicitations by certain methods of delivery but not other methods of delivery. However, one of the alternatives must allow the consumer to prohibit all marketing solicitations from all of the affiliates that are covered by the notice.

(5) *Special rule for a notice following termination of all continuing relationships*—(i) *In general.* A consumer must be given a new opt out notice if, after all continuing relationships with you or your affiliate(s) are terminated, the consumer subsequently establishes another continuing relationship with you or your affiliate(s) and the consumer's eligibility information is to be used to make a marketing solicitation. The new opt out notice must apply, at a minimum, to eligibility information obtained in connection with the new continuing relationship. Consistent

with paragraph (b) of this section, the consumer's decision not to opt out after receiving the new opt out notice would not override a prior opt out election by the consumer that applies to eligibility information obtained in connection with a terminated relationship, regardless of whether the new opt out notice applies to eligibility information obtained in connection with the terminated relationship.

(ii) *Example.* A consumer has an advisory contract with a company that is registered with the Commission as both a broker-dealer and an investment adviser, and that is part of an affiliated group. The consumer terminates the advisory contract. One year after terminating the advisory contract, the consumer opens a brokerage account with the same company. The consumer must be given a new notice and opportunity to opt out before the company's affiliates may make marketing solicitations to the consumer using eligibility information obtained by the company in connection with the new brokerage account relationship, regardless of whether the consumer opted out in connection with the advisory contract.

(b) *Duration of opt out.* The election of a consumer to opt out must be effective for a period of at least five years (the ''opt out period'') beginning when the consumer's opt out election is received and implemented, unless the consumer subsequently revokes the opt out in writing or, if the consumer agrees, electronically. An opt out period of more than five years may be established, including an opt out period that does not expire unless revoked by the consumer.

(c) *Time of opt out.* A consumer may opt out at any time.

§ 248.123 Contents of opt out notice; consolidated and equivalent notices.

(a) *Contents of opt out notice*—(1) *In general.* A notice must be clear, conspicuous, and concise, and must accurately disclose:

(i) *The name of the affiliate(s) providing the notice.* If the notice is provided jointly by multiple affiliates and each affiliate shares a common name, such as ''ABC,'' then the notice may indicate that it is being provided by multiple companies with the ABC name or multiple companies in the ABC group or family of companies, for example, by stating that the notice is provided by ''all of the ABC companies,'' ''the ABC banking, credit card, insurance, and securities companies,'' or by listing the name of each affiliate providing the notice. But if the affiliates providing the joint notice do not all share a common name, then the notice must either separately identify each affiliate by name or identify each of the common names used by those affiliates, for example, by stating that the notice is provided by ''all of the ABC and XYZ companies'' or by ''the ABC bank and securities companies and the XYZ insurance companies'';

(ii) A list of the affiliates or types of affiliates whose use of eligibility information is covered by the notice, which may include companies that become affiliates after the notice is provided to the consumer. If each affiliate covered by the notice shares a common name, such as ''ABC,'' then the notice may indicate that it applies to multiple companies with the ABC name or multiple companies in the ABC group or family of companies, for example, by stating that the notice is provided by ''all of the ABC companies,'' ''the ABC banking, credit card, insurance, and securities companies,'' or by listing the name of each affiliate providing the notice. But if the affiliates covered by the notice do not all share a common name, then the notice must either separately identify each covered affiliate by name or identify each of the common names used by those affiliates, for example, by stating that the notice applies to ''all of the ABC and XYZ companies'' or to ''the ABC banking and securities companies and the XYZ insurance companies'';

(iii) A general description of the types of eligibility information that may be used to make marketing solicitations to the consumer;

(iv) That the consumer may elect to limit the use of eligibility information to make marketing solicitations to the consumer;

(v) That the consumer's election will apply for the specified period of time stated in the notice and, if applicable,

that the consumer will be allowed to renew the election once that period expires;

(vi) If the notice is provided to consumers who may have previously opted out, such as if a notice is provided to consumers annually, that the consumer who has chosen to limit marketing solicitations does not need to act again until the consumer receives a renewal notice; and

(vii) A reasonable and simple method for the consumer to opt out.

(2) *Joint relationships.* (i) If two or more consumers jointly obtain a product or service, a single opt out notice may be provided to the joint consumers. Any of the joint consumers may exercise the right to opt out.

(ii) The opt out notice must explain how an opt out direction by a joint consumer will be treated. An opt out direction by a joint consumer may be treated as applying to all of the associated joint consumers, or each joint consumer may be permitted to opt out separately. If each joint consumer is permitted to opt out separately, one of the joint consumers must be permitted to opt out on behalf of all of the joint consumers and the joint consumers must be permitted to exercise their separate rights to opt out in a single response.

(iii) It is impermissible to require all joint consumers to opt out before implementing any opt out direction.

(3) *Alternative contents.* If the consumer is afforded a broader right to opt out of receiving marketing than is required by this subpart, the requirements of this section may be satisfied by providing the consumer with a clear, conspicuous, and concise notice that accurately discloses the consumer's opt out rights.

(4) *Model notices.* Model notices are provided in the Appendix to this subpart.

(b) *Coordinated and consolidated notices.* A notice required by this subpart may be coordinated and consolidated with any other notice or disclosure required to be issued under any other provision of law by the entity providing the notice, including but not limited to the notice described in section 603(d)(2)(A)(iii) of the FCRA (15 U.S.C. 1681a(d)(2)(A)(iii)) and the GLBA privacy notice.

(c) *Equivalent notices.* A notice or other disclosure that is equivalent to the notice required by this subpart, and that is provided to a consumer together with disclosures required by any other provision of law, satisfies the requirements of this section.

§ 248.124 Reasonable opportunity to opt out.

(a) *In general.* You must not use eligibility information that you receive from an affiliate to make marketing solicitations to a consumer about your products or services unless the consumer is provided a reasonable opportunity to opt out, as required by § 248.121(a)(1)(ii).

(b) *Examples of a reasonable opportunity to opt out.* The consumer is given a reasonable opportunity to opt out if:

(1) *By mail.* The opt out notice is mailed to the consumer. The consumer is given 30 days from the date the notice is mailed to elect to opt out by any reasonable means.

(2) *By electronic means.* (i) The opt out notice is provided electronically to the consumer, such as by posting the notice at an Internet Web site at which the consumer has obtained a product or service. The consumer acknowledges receipt of the electronic notice. The consumer is given 30 days after the date the consumer acknowledges receipt to elect to opt out by any reasonable means.

(ii) The opt out notice is provided to the consumer by e-mail where the consumer has agreed to receive disclosures by e-mail from the person sending the notice. The consumer is given 30 days after the e-mail is sent to elect to opt out by any reasonable means.

(3) *At the time of an electronic transaction.* The opt out notice is provided to the consumer at the time of an electronic transaction, such as a transaction conducted on an Internet Web site. The consumer is required to decide, as a necessary part of proceeding with the transaction, whether to opt out before completing the transaction. There is a simple process that the consumer may use to opt out at that time using the same mechanism through which the transaction is conducted.

(4) *At the time of an in-person transaction.* The opt out notice is provided to the consumer in writing at the time of an in-person transaction. The consumer is required to decide, as a necessary part of proceeding with the transaction, whether to opt out before completing the transaction, and is not permitted to complete the transaction without making a choice. There is a simple process that the consumer may use during the course of the in-person transaction to opt out, such as completing a form that requires consumers to write a ''yes'' or ''no'' to indicate their opt out preference or that requires the consumer to check one of two blank check boxes—one that allows consumers to indicate that they want to opt out and one that allows consumers to indicate that they do not want to opt out.

(5) *By including in a privacy notice.* The opt out notice is included in a GLBA privacy notice. The consumer is allowed to exercise the opt out within a reasonable period of time and in the same manner as the opt out under that privacy notice.

§ 248.125 Reasonable and simple methods of opting out.

(a) *In general.* You must not use eligibility information about a consumer that you receive from an affiliate to make a marketing solicitation to the consumer about your products or services, unless the consumer is provided a reasonable and simple method to opt out, as required by § 248.121(a)(1)(ii).

(b) *Examples*—(1) *Reasonable and simple opt out methods.* Reasonable and simple methods for exercising the opt out right include:

(i) Designating a check-off box in a prominent position on the opt out form;

(ii) Including a reply form and a self-addressed envelope together with the opt out notice;

(iii) Providing an electronic means to opt out, such as a form that can be electronically mailed or processed at an Internet Web site, if the consumer agrees to the electronic delivery of information;

(iv) Providing a toll-free telephone number that consumers may call to opt out; or

(v) Allowing consumers to exercise all of their opt out rights described in a consolidated opt out notice that includes the GLBA privacy, FCRA affiliate sharing, and FCRA affiliate marketing opt outs, by a single method, such as by calling a single toll-free telephone number.

(2) *Opt out methods that are not reasonable and simple.* Reasonable and simple methods for exercising an opt out right *do not* include:

(i) Requiring the consumer to write his or her own letter;

(ii) Requiring the consumer to call or write to obtain a form for opting out, rather than including the form with the opt out notice; or

(iii) Requiring the consumer who receives the opt out notice in electronic form only, such as through posting at an Internet Web site, to opt out solely by paper mail or by visiting a different Web site without providing a link to that site.

(c) *Specific opt out means.* Each consumer may be required to opt out through a specific means, as long as that means is reasonable and simple for that consumer.

§ 248.126 Delivery of opt out notices.

(a) *In general.* The opt out notice must be provided so that each consumer can reasonably be expected to receive actual notice. For opt out notices provided electronically, the notice may be provided in compliance with either the electronic disclosure provisions in this subpart or the provisions in section 101 of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001, *et seq.*

(b) *Examples of reasonable expectation of actual notice.* A consumer may reasonably be expected to receive actual notice if the affiliate providing the notice:

(1) Hand-delivers a printed copy of the notice to the consumer;

(2) Mails a printed copy of the notice to the last known mailing address of the consumer;

(3) Provides a notice by e-mail to a consumer who has agreed to receive electronic disclosures by e-mail from the affiliate providing the notice; or

(4) Posts the notice on the Internet Web site at which the consumer obtained a product or service electronically and requires the consumer to acknowledge receipt of the notice.

(c) *Examples of no reasonable expectation of actual notice.* A consumer may not reasonably be expected to receive actual notice if the affiliate providing the notice:

(1) Only posts the notice on a sign in a branch or office or generally publishes the notice in a newspaper;

(2) Sends the notice by e-mail to a consumer who has not agreed to receive electronic disclosures by e-mail from the affiliate providing the notice; or

(3) Posts the notice on an Internet Web site without requiring the consumer to acknowledge receipt of the notice.

§ 248.127 Renewal of opt out elections.

(a) *Renewal notice and opt out requirement*—(1) *In general.* After the opt out period expires, you may not make marketing solicitations to a consumer who previously opted out, unless:

(i) The consumer has been given a renewal notice that complies with the requirements of this section and §§ 248.124 through 248.126, and a reasonable opportunity and a reasonable and simple method to renew the opt out, and the consumer does not renew the opt out; or

(ii) An exception in § 248.121(c) applies.

(2) *Renewal period.* Each opt out renewal must be effective for a period of at least five years as provided in § 248.122(b).

(3) *Affiliates who may provide the notice.* The notice required by this paragraph must be provided:

(i) By the affiliate that provided the previous opt out notice, or its successor; or

(ii) As part of a joint renewal notice from two or more members of an affiliated group of companies, or their successors, that jointly provided the previous opt out notice.

(b) *Contents of renewal notice.* The renewal notice must be clear, conspicuous, and concise, and must accurately disclose:

(1) The name of the affiliate(s) providing the notice. If the notice is provided jointly by multiple affiliates and each affiliate shares a common name, such as ''ABC,'' then the notice may indicate it is being provided by multiple companies with the ABC name or multiple companies in the ABC group or family of companies, for example, by stating that the notice is provided by ''all of the ABC companies,'' ''the ABC banking, credit card, insurance, and securities companies,'' or by listing the name of each affiliate providing the notice. But if the affiliates providing the joint notice do not all share a common name, then the notice must either separately identify each affiliate by name or identify each of the common names used by those affiliates, for example, by stating that the notice is provided by ''all of the ABC and XYZ companies'' or by ''the ABC banking and securities companies and the XYZ insurance companies'';

(2) A list of the affiliates or types of affiliates whose use of eligibility information is covered by the notice, which may include companies that become affiliates after the notice is provided to the consumer. If each affiliate covered by the notice shares a common name, such as ''ABC,'' then the notice may indicate that it applies to multiple companies with the ABC name or multiple companies in the ABC group or family of companies, for example, by stating that the notice is provided by ''all of the ABC companies,'' ''the ABC banking, credit card, insurance, and securities companies,'' or by listing the name of each affiliate providing the notice. But if the affiliates covered by the notice do not all share a common name, then the notice must either separately identify each covered affiliate by name or identify each of the common names used by those affiliates, for example, by stating that the notice applies to ''all of the ABC and XYZ companies'' or to ''the ABC banking and securities companies and the XYZ insurance companies'';

(3) A general description of the types of eligibility information that may be used to make marketing solicitations to the consumer;

(4) That the consumer previously elected to limit the use of certain information to make marketing solicitations to the consumer;

(5) That the consumer's election has expired or is about to expire;

(6) That the consumer may elect to renew the consumer's previous election;

(7) If applicable, that the consumer's election to renew will apply for the specified period of time stated in the notice and that the consumer will be allowed to renew the election once that period expires; and

(8) A reasonable and simple method for the consumer to opt out.

(c) *Timing of the renewal notice*—(1) *In general.* A renewal notice may be provided to the consumer either:

(i) A reasonable period of time before the expiration of the opt out period; or

(ii) Any time after the expiration of the opt out period but before marketing solicitations that would have been prohibited by the expired opt out are made to the consumer.

(2) *Combination with annual privacy notice.* If you provide an annual privacy notice under the GLBA, providing a renewal notice with the last annual privacy notice provided to the consumer before expiration of the opt out period is a reasonable period of time before expiration of the opt out in all cases.

(d) *No effect on opt out period.* An opt out period may not be shortened by sending a renewal notice to the consumer before expiration of the opt out period, even if the consumer does not renew the opt out.

§ 248.128 Effective date, compliance date, and prospective application.

(a) *Effective date.* This subpart is effective September 10, 2009.

(b) *Mandatory compliance date.* Compliance with this subpart is required not later than January 1, 2010.

(c) *Prospective application.* The provisions of this subpart do not prohibit you from using eligibility information that you receive from an affiliate to make a marketing solicitation to a consumer if you receive such information prior to January 1, 2010. For purposes of this section, you are deemed to receive eligibility information when such information is placed into a common database and is accessible by you.

APPENDIX TO SUBPART B OF PART 248—MODEL FORMS

a. Although you and your affiliates are not required to use the model forms in this Appendix, use of a model form (if applicable to each person that uses it) complies with the requirement in section 624 of the FCRA for clear, conspicuous, and concise notices.

b. Although you may need to change the language or format of a model form to reflect your actual policies and procedures, any such changes may not be so extensive as to affect the substance, clarity, or meaningful sequence of the language in the model forms. Acceptable changes include, for example:

1. Rearranging the order of the references to ''your income,'' ''your account history,'' and ''your credit score.''

2. Substituting other types of information for ''income,'' ''account history,'' or ''credit score'' for accuracy, such as ''payment history,'' ''credit history,'' ''payoff status,'' or ''claims history.''

3. Substituting a clearer and more accurate description of the affiliates providing or covered by the notice for phrases such as ''the [ABC] group of companies.''

4. Substituting other types of affiliates covered by the notice for ''credit card,'' ''insurance,'' or ''securities'' affiliates.

5. Omitting items that are not accurate or applicable. For example, if a person does not limit the duration of the opt out period, the notice may omit information about the renewal notice.

6. Adding a statement informing the consumer how much time they have to opt out before shared eligibility information may be used to make solicitations to them.

7. Adding a statement that the consumer may exercise the right to opt out at any time.

8. Adding the following statement, if accurate: ''If you previously opted out, you do not need to do so again.''

9. Providing a place on the form for the consumer to fill in identifying information, such as his or her name and address.

10. Adding disclosures regarding the treatment of opt-outs by joint consumers to comply with § 248.123(a)(2), if applicable.

A–1—MODEL FORM FOR INITIAL OPT OUT NOTICE (SINGLE-AFFILIATE NOTICE)—[YOUR CHOICE TO LIMIT MARKETING]/[MARKETING OPT OUT]

• [Name of Affiliate] is providing this notice.

• [Optional: Federal law gives you the right to limit some but not all marketing from our affiliates. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from our affiliates.]

• You may limit our affiliates in the [ABC] group of companies, such as our [investment adviser, broker, transfer agent, and investment company] affiliates, from marketing their products or services to you based on your personal information that we collect and share with them. This information includes your [income], your [account history with us], and your [credit score].

• Your choice to limit marketing offers from our affiliates will apply [until you tell us to change your choice]/[for x years from when you tell us your choice]/[for at least 5 years from when you tell us your choice]. [Include if the opt out period expires.] Once that period expires, you will receive a renewal notice that will allow you to continue to limit marketing offers from our affiliates for [another x years]/[at least another 5 years].

• [Include, if applicable, in a subsequent notice, including an annual notice, for consumers who may have previously opted out.] If you have already made a choice to limit marketing offers from our affiliates, you do not need to act again until you receive the renewal notice.

To limit marketing offers, contact us [include all that apply]:

• By telephone: 1–877–###–####

• On the Web: *www.—.com*

• By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Do not allow your affiliates to use my personal information to market to me.

A–2—MODEL FORM FOR INITIAL OPT OUT NOTICE (JOINT NOTICE)—[YOUR CHOICE TO LIMIT MARKETING]/[MARKETING OPT OUT]

• The [ABC group of companies] is providing this notice.

• [Optional: Federal law gives you the right to limit some but not all marketing from the [ABC] companies. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from the [ABC] companies.]

• You may limit the [ABC] companies, such as the [ABC investment companies, investment advisers, transfer agents, and broker-dealers] affiliates, from marketing their products or services to you based on your personal information that they receive from other [ABC] companies. This information includes your [income], your [account history], and your [credit score].

• Your choice to limit marketing offers from the [ABC] companies will apply [until you tell us to change your choice]/[for x years from when you tell us your choice]/[for at least 5 years from when you tell us your choice]. [Include if the opt out period expires.] Once that period expires, you will receive a renewal notice that will allow you to continue to limit marketing offers from the [ABC] companies for [another x years]/[at least another 5 years].

• [Include, if applicable, in a subsequent notice, including an annual notice, for consumers who may have previously opted out.] If you have already made a choice to limit marketing offers from the [ABC] companies, you do not need to act again until you receive the renewal notice.

To limit marketing offers, contact us [include all that apply]:

• By telephone: 1–877–###–####

• On the Web: *www.—.com*

• By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Do not allow any company [in the ABC group of companies] to use my personal information to market to me.

A–3—MODEL FORM FOR RENEWAL NOTICE (SINGLE-AFFILIATE NOTICE)—[RENEWING YOUR CHOICE TO LIMIT MARKETING]/[RENEWING YOUR MARKETING OPT OUT]

• [Name of Affiliate] is providing this notice.

• [Optional: Federal law gives you the right to limit some but not all marketing from our affiliates. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from our affiliates.]

• You previously chose to limit our affiliates in the [ABC] group of companies, such

as our [investment adviser, investment company, transfer agent, and broker-dealer] affiliates, from marketing their products or services to you based on your personal information that we share with them. This information includes your [income], your [account history with us], and your [credit score].

• Your choice has expired or is about to expire.

To renew your choice to limit marketing for [x] more years, contact us [include all that apply]:

• By telephone: 1–877–###–####
• On the Web: *www.—.com*
• By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Renew my choice to limit marketing for [x] more years.

A–4—MODEL FORM FOR RENEWAL NOTICE (JOINT NOTICE)—[RENEWING YOUR CHOICE TO LIMIT MARKETING]/[RENEWING YOUR MARKETING OPT OUT]

• The [ABC group of companies] is providing this notice.

• [Optional: Federal law gives you the right to limit some but not all marketing from the [ABC] companies. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from the [ABC] companies.]

• You previously chose to limit the [ABC] companies, such as the [ABC investment adviser, investment company, transfer agent, and broker-dealer] affiliates, from marketing their products or services to you based on your personal information that they receive from other ABC companies. This information includes your [income], your [account history], and your [credit score].

• Your choice has expired or is about to expire.

To renew your choice to limit marketing for [x] more years, contact us [include all that apply]:

• By telephone: 1–877–###–####
• On the Web: *www.—.com*
• By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Renew my choice to limit marketing for [x] more years.

A–5—MODEL FORM FOR VOLUNTARY ''NO MARKETING'' NOTICE—YOUR CHOICE TO STOP MARKETING

• [Name of Affiliate] is providing this notice.

• You may choose to stop all marketing from us and our affiliates.

• [Your choice to stop marketing from us and our affiliates will apply until you tell us to change your choice.]

To stop all marketing, contact us [include all that apply]:

• By telephone: 1–877–###–####
• On the Web: *www.—.com*
• By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Do not market to me.

Subpart C—Regulation S–ID: Identity Theft Red Flags

SOURCE: 78 FR 23663, Apr. 17, 2013, unless otherwise noted.

§ 248.201 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to a *financial institution* or *creditor*, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681), that is:

(1) A broker, dealer or any other person that is registered or required to be registered under the Securities Exchange Act of 1934;

(2) An investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act; or

(3) An investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940.

(b) *Definitions.* For purposes of this subpart, and Appendix A of this subpart, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes a brokerage account, a *mutual fund* account (*i.e.*, an account with an open-end investment company), and an investment advisory account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign financial institution or

creditor, the managing official of that branch or agency; and

(ii) In the case of a financial institution or creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681m(e)(4).

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identifying information* means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—

(i) Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(iii) Unique electronic identification number, address, or routing code; or

(iv) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

(9) *Identity theft* means a fraud committed or attempted using the identifying information of another person without authority.

(10) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(11) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(12) *Other definitions.*

(i) *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)).

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

(iii) *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)).

(iv) *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)).

(v) *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.

(vi) Other terms not defined in this subpart have the same meaning as in the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(c) *Periodic identification of covered accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program—*

(1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of

a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A to this subpart and include in its Program those guidelines that are appropriate.

§ 248.202 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 248.201(a) that issues a credit or debit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a *credit card* or *debit card* as defined in 15 U.S.C. 1681a(r).

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(3) Other terms not defined in this subpart have the same meaning as in the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(c) *Address validation requirements.* A card issuer must establish and implement reasonable written policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 248.201.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or

(c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and be provided separately from its regular correspondence with the cardholder.

APPENDIX A TO SUBPART C OF PART 248—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 248.201 requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §248.201(b)(3), to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of §248.201.

I. THE PROGRAM

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. IDENTIFYING RELEVANT RED FLAGS

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable regulatory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. DETECTING RED FLAGS

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(*l*) (31 CFR 1023.220 (broker-dealers) and 1024.220 (mutual funds)); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with §248.201; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with §248.201.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A to this subpart, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings From a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as referenced in Sec. 605(h) of the Fair Credit Reporting Act (15 U.S.C. 1681c(h)).

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement means of accessing the account or for the addition of an authorized user on the account.

20. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns; or

d. A material change in electronic fund transfer patterns in connection with a deposit account.

21. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

22. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

23. The financial institution or creditor is notified that the customer is not receiving paper account statements.

24. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

25. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

PART 249—FORMS, SECURITIES EXCHANGE ACT OF 1934

Sec.

Subpart A—Forms for Registration or Exemption of, and Notification of Action Taken by, National Securities Exchanges

Subpart B—Forms for Reports To Be Filed by Officers, Directors, and Security Holders

Subpart C—Forms for Applications for Registration of Securities on National Securities Exchanges and Similar Matters

Forms for Annual and Other Reports of Issuers and Other Persons Required Under Sections 13, 14A, and 15(d) of the Securities Exchange Act of 1934