AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PART 40—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.
40.1 Purpose and scope.
40.2 Model privacy form and examples.
40.3 Definitions.

Subpart A—Privacy and Opt Out Notices

40.4 Initial privacy notice to consumers required.
40.5 Annual privacy notice to customers required.
40.6 Information to be included in privacy notices.
40.7 Form of opt out notice to consumers; opt out methods.
40.8 Revised privacy notices.
40.9 Delivering privacy and opt out notices.

Subpart B—Limits on Disclosures

40.10 Limitation on disclosure of nonpublic personal information to nonaffiliated third parties.
40.11 Limits on redisclosure and reuse of information.
40.12 Limits on sharing account number information for marketing purposes.

Subpart C—Exceptions

40.13 Exception to opt out requirements for service providers and joint marketing.
40.14 Exceptions to notice and opt out requirements for processing and servicing transactions.
40.15 Other exceptions to notice and opt out requirements.

Subpart D—Relation to Other Laws; Effective Date

40.16 Protection of Fair Credit Reporting Act.
40.17 Relation to State laws.
40.18 Effective date; transition rule.

APPENDIX A TO PART 40—MODEL PRIVACY FORM

APPENDIX B TO PART 40—SAMPLE CLAUSES

AUTHORITY: 12 U.S.C. 93a; 15 U.S.C. 6801 *et seq.*

SOURCE: 65 FR 35196, June 1, 2000, unless otherwise noted.

§40.1 Purpose and scope.

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

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

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

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§40.13, 40.14, and 40.15.

(b) *Scope.* (1) This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to United States offices of entities for which the Office of the Comptroller of the Currency has primary supervisory authority. They are referred to in this part as "the bank." These are national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities except a broker or dealer that is registered under the Securities Exchange Act of 1934, a registered investment adviser (with respect to the investment advisory activities of the adviser and activities incidental to those investment advisory activities), an investment company registered under the Investment Company Act of 1940, an insurance company that is subject to supervision by a State insurance regulator (with respect to insurance activities of the company and activities incidental to those insurance activities), and an entity that is subject to regulation by the Commodity Futures Trading Commission.

(2) Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability

and Accountability Act of 1996 (42 U.S.C. 1320d–1320d–8).

[65 FR 35196, June 1, 2000, as amended at 73 FR 22252, Apr. 24, 2008]

§ 40.2 Model privacy form and examples.

(a) *Model privacy form.* Use of the model privacy form in Appendix A of this part, consistent with the instructions in Appendix A, constitutes compliance with the notice content requirements of §§ 40.6 and 40.7 of this part, although use of the model privacy form is not required.

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

[74 FR 62916, Dec. 1, 2009]

§ 40.3 Definitions.

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

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

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

(2) *Examples.* (i) *Reasonably understandable.* A bank makes its notice reasonably understandable if it:

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

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

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

(D) Avoids multiple negatives;

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

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

(ii) *Designed to call attention.* A bank designs its notice to call attention to the nature and significance of the information in it if the bank:

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

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

(C) Provides wide margins and ample line spacing;

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

(E) In a form that combines the bank's notice with other information, uses 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 a bank provides a notice on a web page, the bank designs its notice to call attention to the nature and significance of the information in it if the bank uses 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 the bank either:

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

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

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

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

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

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

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

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

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

(v) An individual who is a consumer of another financial institution is not a bank's consumer solely because the bank acts as agent for, or provides processing or other services to, that financial institution.

(vi) An individual is not a bank's consumer solely because he or she has designated the bank as trustee for a trust.

(vii) An individual is not a bank's consumer solely because he or she is a beneficiary of a trust for which the bank is a trustee.

(viii) An individual is not a bank's consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that the bank sponsors or for which the bank acts as a trustee or fiduciary.

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

(g) *Control* of a company means:

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

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

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

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

(i)(1) *Customer relationship* means a continuing relationship between a consumer and a bank under which the bank provides 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 a bank if the consumer:

(A) Has a deposit or investment account with the bank;

(B) Obtains a loan from the bank;

(C) Has a loan for which you own the servicing rights;

(D) Purchases an insurance product from the bank;

(E) Holds an investment product through the bank, such as when the bank acts as a custodian for securities or for assets in an Individual Retirement Arrangement;

(F) Enters into an agreement or understanding with the bank whereby the bank undertakes to arrange or broker a home mortgage loan for the consumer;

(G) Enters into a lease of personal property with the bank; or

(H) Obtains financial, investment, or economic advisory services from the bank for a fee.

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

(A) The consumer obtains a financial product or service only in isolated transactions, such as using the bank's ATM to withdraw cash from an account at another financial institution or purchasing a cashier's check or money order;

(B) The bank sells the consumer's loan and does not retain the rights to service that loan; or

(C) The bank sells the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions.

(j) *Federal functional regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board; and

(6) The Securities and Exchange Commission.

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

(2) *Financial institution* does not include:

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

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

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

(l)(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 a bank's evaluation or brokerage of information that the bank collects in connection with a request or an application from a consumer for a financial product or service.

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

(i) A bank's affiliate; or

(ii) A person employed jointly by a bank and any company that is not the bank's 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 a bank's (or its 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 of 1956 (12 U.S.C. 1843(k)(4)(H) and (I)).

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

(i) Personally identifiable financial information; and

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

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

(i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or

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

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

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

the list is a consumer of a financial institution.

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

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

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

(iii) The bank otherwise obtains 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 a bank 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 the bank's customers or has obtained a financial product or service from the bank;

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

(E) Any information that a consumer provides to a bank or that the bank or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(F) Any information the bank collects through an Internet "cookie" (an information collecting device from a web server); and

(G) Information from a consumer report.

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

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

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

(p)(1) *Publicly available information* means any information that a bank has a reasonable basis to believe is lawfully made available to the general public from:

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

(ii) Widely distributed media; or

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

(2) *Reasonable basis.* A bank has a reasonable basis to believe that information is lawfully made available to the general public if the bank has taken steps to determine:

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

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

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

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

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

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

Subpart A—Privacy and Opt Out Notices

§ 40.4 Initial privacy notice to consumers required.

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

(1) *Customer.* An individual who becomes the bank's customer, not later than when the bank establishes a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before the bank discloses any nonpublic personal information about the consumer to any nonaffiliated third party, if the bank makes such a disclosure other than as authorized by §§ 40.14 and 40.15.

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

(1) The bank does not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 40.14 and 40.15; and

(2) The bank does not have a customer relationship with the consumer.

(c) *When the bank establishes a customer relationship*—(1) *General rule.* A bank establishes a customer relationship when it and the consumer enter into a continuing relationship.

(2) *Special rule for loans.* A bank establishes a customer relationship with a consumer when the bank originates a loan to the consumer for personal, family, or household purposes. If the bank subsequently transfers the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3)(i) *Examples of establishing customer relationship.* A bank establishes a customer relationship when the consumer:

(A) Opens a credit card account with the bank;

(B) Executes the contract to open a deposit account with the bank, obtains credit from the bank, or purchases insurance from the bank;

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

(D) Becomes the bank's client for the purpose of the bank's providing credit counseling or tax preparation services.

(ii) *Examples of loan rule.* A bank establishes a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when the bank:

(A) Originates the loan to the consumer; or

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

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

(1) The bank may provide a revised privacy notice, under § 40.8, that covers the customer's new financial product or service; or

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

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

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

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

(2) *Examples of exceptions.* (i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if a bank acquires a customer's deposit liability or the servicing rights to a customer's loan from another financial institution and the customer does not have a choice about the bank's acquisition.

(ii) *Substantial delay of customer's transaction.* Providing notice not later

than when a bank establishes a customer relationship would substantially delay the customer's transaction when:

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

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

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

(f) *Delivery*. When a bank is required to deliver an initial privacy notice by this section, the bank must deliver it according to §40.9. If the bank uses a short-form initial notice for non-customers according to §40.6(d), the bank may deliver its privacy notice according to §40.6(d)(3).

§40.5 Annual privacy notice to customers required.

(a)(1) *General rule*. A bank must provide a clear and conspicuous notice to customers that accurately reflects its 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. A bank may define the 12-consecutive-month period, but the bank must apply it to the customer on a consistent basis.

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

(b)(1) *Termination of customer relationship*. A bank is not required to provide an annual notice to a former customer.

(2) *Examples*. A bank's customer becomes a former customer when:

(i) In the case of a deposit account, the account is inactive under the bank's policies;

(ii) In the case of a closed-end loan, the customer pays the loan in full, the bank charges off the loan, or the bank sells the loan without retaining servicing rights;

(iii) In the case of a credit card relationship or other open-end credit relationship, the bank no longer provides any statements or notices to the customer concerning that relationship or the bank sells the credit card receivables without retaining servicing rights; or

(iv) The bank has not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material.

(c) *Special rule for loans*. If a bank does not have a customer relationship with a consumer under the special rule for loans in §40.4(c)(2), then the bank need not provide an annual notice to that consumer under this section.

(d) *Delivery*. When a bank is required to deliver an annual privacy notice by this section, the bank must deliver it according to §40.9.

§40.6 Information to be included in privacy notices.

(a) *General rule*. The initial, annual, and revised privacy notices that a bank provides under §§40.4, 40.5, and 40.8 must include each of the following items of information, in addition to any other information the bank wishes to provide, that applies to the bank and to the consumers to whom the bank sends its privacy notice:

(1) The categories of nonpublic personal information that the bank collects;

(2) The categories of nonpublic personal information that the bank discloses;

(3) The categories of affiliates and nonaffiliated third parties to whom the

bank discloses nonpublic personal information, other than those parties to whom the bank discloses information under §§ 40.14 and 40.15;

(4) The categories of nonpublic personal information about the bank's former customers that the bank discloses and the categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information about the bank's former customers, other than those parties to whom the bank discloses information under §§ 40.14 and 40.15;

(5) If a bank discloses nonpublic personal information to a nonaffiliated third party under § 40.13 (and no other exception in §§ 40.14 or 40.15 applies to that disclosure), a separate statement of the categories of information the bank discloses and the categories of third parties with whom the bank has contracted;

(6) An explanation of the consumer's right under § 40.10(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 the bank makes 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) The bank's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that the bank makes 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 §§ 40.14 and 40.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 40.4 and 40.5. 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 the bank collects.* A bank satisfies the requirement to categorize the nonpublic personal information that it collects if it lists the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with the bank or its 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 the bank discloses.* (i) A bank satisfies the requirement to categorize the nonpublic personal information that it discloses if the bank lists 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 a bank reserves the right to disclose all of the nonpublic personal information about consumers that it collects, it may simply state that fact without describing the categories or examples of the nonpublic personal information it discloses.

(3) *Categories of affiliates and nonaffiliated third parties to whom the bank discloses.* A bank satisfies the requirement to categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic personal information if the bank lists 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 a bank discloses nonpublic personal information under the exception in § 40.13 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the bank satisfies the disclosure requirement of paragraph (a)(5) of this section if it:

(i) Lists the categories of nonpublic personal information it discloses, using the same categories and examples the bank used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) States whether the third party is:

(A) A service provider that performs marketing services on the bank's behalf or on behalf of the bank and another financial institution; or

(B) A financial institution with whom the bank has a joint marketing agreement.

(5) *Simplified notices.* If a bank does not disclose, and does not wish to reserve the right to disclose, nonpublic personal information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under §§40.14 and 40.15, the bank may simply state that fact, in addition to the information it must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

(6) *Confidentiality and security.* A bank describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if it does both of the following:

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

(ii) States whether the bank has security practices and procedures in place to ensure the confidentiality of the information in accordance with the bank's policy. The bank is not required to describe technical information about the safeguards it uses.

(d) *Short-form initial notice with opt out notice for non-customers.* (1) A bank may satisfy the initial notice requirements in §§40.4(a)(2), 40.7(b), and 40.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as the bank delivers an opt out notice as required in §40.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that the bank's privacy notice is available upon request; and

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

(3) The bank must deliver its short-form initial notice according to §40.9. The bank is not required to deliver its privacy notice with its short-form initial notice. The bank instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the bank's short-form notice requests the bank's privacy notice, the bank must deliver its privacy notice according to §40.9.

(4) *Examples of obtaining privacy notice.* The bank provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the bank:

(i) Provides 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 the bank's office, maintain copies of the notice on hand that the bank provides to the consumer immediately upon request.

(e) *Future disclosures.* The bank's notice may include:

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

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

(f) *Model privacy form.* Pursuant to §40.2(a) of this part, a model privacy form that meets the notice content requirements of this section is included in Appendix A of this part.

(g) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix B of this part. Use of a sample clause in a privacy notice provided on or before December 31, 2010, to the extent applicable, constitutes compliance with this part.

[65 FR 35196, June 1, 2000, as amended at 74 FR 62916, Dec. 1, 2009]

EFFECTIVE DATE NOTE: At 74 FR 62916, Dec. 1, 2009, §40.6 was amended by adding (g) which is effective until January 1, 2012.

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

(a) (1) *Form of opt out notice.* If a bank is required to provide an opt out notice under §40.10(a), it must provide a clear and conspicuous notice to each of its consumers that accurately explains the

right to opt out under that section. The notice must state:

(i) That the bank discloses or reserves the right to disclose nonpublic personal information about its 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.* A bank provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the bank:

(A) Identifies all of the categories of nonpublic personal information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the bank discloses the information, as described in § 40.6(a)(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

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

(ii) *Reasonable opt out means.* A bank provides a reasonable means to exercise an opt out right if it:

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

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

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

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

(iii) *Unreasonable opt out means.* A bank *does 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 the bank provided with the initial notice but did not include with the subsequent notice.

(iv) *Specific opt out means.* A bank 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.* A bank may provide the opt out notice together with or on the same written or electronic form as the initial notice the bank provides in accordance with § 40.4.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If a bank provides the opt out notice later than required for the initial notice in accordance with § 40.4, the bank 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 a bank, the bank may provide a single opt out notice. The bank's opt out notice must explain how the bank will treat an opt out direction by a joint consumer (as explained in paragraph (d)(5) of this section).

(2) Any of the joint consumers may exercise the right to opt out. The bank 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 a bank permits each joint consumer to opt out separately, the bank must permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A bank may not require *all* joint consumers to opt out before it implements *any* opt out direction.

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

(i) Send a single opt out notice to John's address, but the bank 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 the bank does so and John opts out, the bank may not require Mary to opt out as well before implementing John's opt out direction.

(iii) Permit John and Mary to make different opt out directions. If the bank does so:

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

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

(C) If John opts out and Mary does not, the bank 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.* A bank must comply with a consumer's opt out direction as soon as reasonably practicable after the bank receives 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 the bank collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the bank, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) *Delivery.* When a bank is required to deliver an opt out notice by this section, the bank must deliver it according to §40.9.

(i) *Model privacy form.* Pursuant to §40.2(a) of this part, a model privacy form that meets the notice content requirements of this section is included in Appendix A of this part.

[65 FR 35196, June 1, 2000, as amended at 74 FR 62916, Dec. 1, 2009]

§40.8 Revised privacy notices.

(a) *General rule.* Except as otherwise authorized in this part, a bank 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 the bank provided to that consumer under §40.4, unless:

(1) The bank has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The bank has provided to the consumer a new opt out notice;

(3) The bank has given the consumer a reasonable opportunity, before the bank discloses 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 §§40.13, 40.14, and 40.15, a bank must provide a revised notice before it:

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

(ii) Discloses 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 the bank discloses nonpublic personal information to a new nonaffiliated third party that the bank adequately described in its prior notice.

(c) *Delivery.* When a bank is required to deliver a revised privacy notice by this section, the bank must deliver it according to §40.9.

§40.9 Delivering privacy and opt out notices.

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

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

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

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

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

(iv) For an isolated transaction with the consumer, such as an ATM transaction, posts the notice on the ATM screen and requires 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.* A bank may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

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

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

(c) *Annual notices only.* A bank may reasonably expect that a customer will receive actual notice of the bank's annual privacy notice if:

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

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

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

(e) *Retention or accessibility of notices for customers.* (1) For customers only, a bank must provide the initial notice required by § 40.4(a)(1), the annual notice required by § 40.5(a), and the revised notice required by § 40.8 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.* A bank provides a privacy notice to the customer so that the customer can retain it or obtain it later if the bank:

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

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

(iii) Makes its 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.* A bank may provide a joint notice from it and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the bank and the other institutions.

(g) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from a bank, the bank may satisfy the initial, annual, and revised notice requirements of §§ 40.4(a), 40.5(a), and 40.8(a), respectively, by providing one notice to those consumers jointly.

Subpart B—Limits on Disclosures

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

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

(i) The bank has provided to the consumer an initial notice as required under § 40.4;

(ii) The bank has provided to the consumer an opt out notice as required in § 40.7;

(iii) The bank has given the consumer a reasonable opportunity, before it discloses 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 the bank not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§40.13, 40.14, and 40.15.

(3) *Examples of reasonable opportunity to opt out*. A bank provides a consumer with a reasonable opportunity to opt out if:

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

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

(iii) *Isolated transaction with consumer*. For an isolated transaction, such as the purchase of a cashier's check by a consumer, a bank provides the consumer with a reasonable opportunity to opt out if the bank provides the notices required in paragraph (a)(1) of this section at the time of the transaction and requests 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) A bank must comply with this section, regardless of whether the bank and the consumer have established a customer relationship.

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

(c) *Partial opt out*. A bank 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.

§40.11 Limits on redisclosure and reuse of information.

(a)(1) *Information the bank receives under an exception*. If a bank receives nonpublic personal information from a nonaffiliated financial institution under an exception in §§40.14 or 40.15 of this part, the bank's disclosure and use of that information is limited as follows:

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

(ii) The bank may disclose the information to its affiliates, but the bank's affiliates may, in turn, disclose and use the information only to the extent that the bank may disclose and use the information; and

(iii) The bank may disclose and use the information pursuant to an exception in §§40.14 or 40.15 in the ordinary course of business to carry out the activity covered by the exception under which the bank received the information.

(2) *Example*. If a bank receives a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in §40.14(a), the bank may disclose that information under any exception in §§40.14 or 40.15 in the ordinary course of business in order to provide those services. For example, the bank could disclose the information in response to a properly authorized subpoena or to its attorneys, accountants, and auditors. The bank could not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.

(b)(1) *Information a bank receives outside of an exception*. If a bank receives nonpublic personal information from a nonaffiliated financial institution other than under an exception in §§40.14 or 40.15 of this part, the bank may disclose the information only:

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

(ii) To its affiliates, but its affiliates may, in turn, disclose the information

only to the extent that the bank 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 the bank received the information.

(2) *Example.* If a bank obtains a customer list from a nonaffiliated financial institution outside of the exceptions in §§ 40.14 and 40.15:

(i) The bank may use that list for its own purposes; and

(ii) The bank may disclose that list to another nonaffiliated third party only if the financial institution from which the bank purchased the list could have lawfully disclosed the list to that third party. That is, the bank may disclose the list in accordance with the privacy policy of the financial institution from which the bank received the list, as limited by the opt out direction of each consumer whose nonpublic personal information the bank intends to disclose and the bank may disclose the list in accordance with an exception in §§ 40.14 or 40.15, such as to the bank's attorneys or accountants.

(c) *Information a bank discloses under an exception.* If a bank discloses nonpublic personal information to a nonaffiliated third party under an exception in §§ 40.14 or 40.15 of this part, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to the bank's 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 §§ 40.14 or 40.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) *Information a bank discloses outside of an exception.* If a bank discloses nonpublic personal information to a nonaffiliated third party other than under an exception in §§ 40.14 or 40.15 of this part, the third party may disclose the information only:

(1) To the bank's affiliates;

(2) To the third party's affiliates, but the third party's 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 the bank made it directly to that person.

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

(a) *General prohibition on disclosure of account numbers.* A bank 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 a bank discloses an account number or similar form of access number or access code:

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

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

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

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

Subpart C—Exceptions

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

(a) *General rule.* (1) The opt out requirements in §§40.7 and 40.10 do not apply when a bank provides nonpublic personal information to a nonaffiliated third party to perform services for the bank or functions on the bank's behalf, if the bank:

(i) Provides the initial notice in accordance with §40.4; and

(ii) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the bank disclosed the information, including use under an exception in §40.14 or 40.15 in the ordinary course of business to carry out those purposes.

(2) *Example.* If a bank discloses nonpublic personal information under this section to a financial institution with which the bank performs joint marketing, the bank's 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 §§40.14 or 40.15 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 a bank under paragraph (a) of this section may include marketing of the bank's own products or services or marketing of financial products or services offered pursuant to joint agreements between the bank 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 a bank and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

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

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in §40.4(a)(2), the opt out in §§40.7 and 40.10 and service providers and joint marketing in §40.13 do not apply if the bank discloses nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

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

(2) Maintaining or servicing the consumer's account with a bank, 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 the bank's 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 a bank or any other party;

(v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's

insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or State law;

(vi) In connection with:

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

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

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

§ 40.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice to consumers in § 40.4(a)(2), the opt out in §§ 40.7 and 40.10, and service providers and joint marketing in § 40.13 do not apply when a bank discloses 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 a bank's 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 a bank, persons that are assessing the bank's compliance with industry standards, and the bank's 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 a bank 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 a bank's disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to the bank for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 40.7(f).

Subpart D—Relation to Other Laws; Effective Date

§ 40.16 Protection of Fair Credit Reporting Act.

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

§ 40.17 Relation to State laws.

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

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

§ 40.18 Effective date; transition rule.

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

(b)(1) *Notice requirement for consumers who are the bank's customers on the compliance date.* By July 1, 2001, a bank must have provided an initial notice, as required by § 40.4, to consumers who are the bank's customers on July 1, 2001.

(2) *Example.* A bank provides an initial notice to consumers who are its customers on July 1, 2001, if, by that date, the bank has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the bank's existing customers.

(c) *Two-year grandfathering of service agreements.* Until July 1, 2002, a contract that a bank has entered into with a nonaffiliated third party to perform services for the bank or functions on the bank's behalf satisfies the provisions of § 40.13(a)(1)(ii) of this part, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the bank entered into the agreement on or before July 1, 2000.

APPENDIX A TO PART 40—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 §§ 40.6 and 40.7 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 §§ 40.14 and 40.15 and with service providers pursuant to § 40.13 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 § 40.13 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 § 40.13 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 12 CFR part 41, subpart C, 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 §§40.7 and 40.10(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 §40.10(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 §40.9(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 §40.6(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 §40.6(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 § 40.13 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.

APPENDIX B TO PART 40—SAMPLE CLAUSES

This Appendix only applies to privacy notices provided before January 1, 2011. Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A–1—CATEGORIES OF INFORMATION A BANK COLLECTS (ALL INSTITUTIONS)

A bank may use this clause, as applicable, to meet the requirement of § 40.6(a)(1) to describe the categories of nonpublic personal information the bank collects.

Sample Clause A–1:

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

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

A–2—CATEGORIES OF INFORMATION A BANK DISCLOSES (INSTITUTIONS THAT DISCLOSE OUTSIDE OF THE EXCEPTIONS)

A bank may use one of these clauses, as applicable, to meet the requirement of § 40.6(a)(2) to describe the categories of nonpublic personal information the bank discloses. The bank may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in §§ 40.13, 40.14, and 40.15.

Sample Clause A–2, Alternative 1:

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

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

Sample Clause A–2, Alternative 2:

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

A–3—CATEGORIES OF INFORMATION A BANK DISCLOSES AND PARTIES TO WHOM THE BANK DISCLOSES (INSTITUTIONS THAT DO NOT DISCLOSE OUTSIDE OF THE EXCEPTIONS)

A bank may use this clause, as applicable, to meet the requirements of §§ 40.6(a)(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that the bank discloses and the categories of affiliates and nonaffiliated third parties to whom the bank discloses. A bank may use this clause if the bank does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in §§ 40.14, and 40.15.

Sample Clause A–3:

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

A–4—CATEGORIES OF PARTIES TO WHOM A BANK DISCLOSES (INSTITUTIONS THAT DISCLOSE OUTSIDE OF THE EXCEPTIONS)

A bank may use this clause, as applicable, to meet the requirement of § 40.6(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information. The bank may use this clause if the bank discloses nonpublic personal information other than as permitted by the exceptions in §§ 40.13, 40.14, and 40.15, as well as when permitted by the exceptions in §§ 40.14 and 40.15.

Sample Clause A–4:

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

• Financial service providers, such as [*provide illustrative examples, such as "mortgage bankers, securities broker-dealers, and insurance agents*"];

• Non-financial companies, such as [*provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers*"]; and

• Others, such as [*provide illustrative examples, such as "non-profit organizations*"].

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

A–5—SERVICE PROVIDER/JOINT MARKETING EXCEPTION

A bank may use one of these clauses, as applicable, to meet the requirements of § 40.6(a)(5) related to the exception for service providers and joint marketers in § 40.13. If a bank discloses nonpublic personal information under this exception, the bank must describe the categories of nonpublic personal information the bank discloses and the categories of third parties with whom the bank has contracted.

Sample Clause A–5, Alternative 1:

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

• Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as "your name, address, social security number, assets, and income*"];

• Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as "your account balance, payment history, parties to transactions, and credit card usage*"]; and

• Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as "your creditworthiness and credit history*"].

Sample Clause A–5, Alternative 2:

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

A–6—EXPLANATION OF OPT OUT RIGHT (INSTITUTIONS THAT DISCLOSE OUTSIDE OF THE EXCEPTIONS)

A bank may use this clause, as applicable, to meet the requirement of § 40.6(a)(6) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The bank may use this clause if the bank discloses nonpublic personal information other than as permitted by the exceptions in §§ 40.13, 40.14, and 40.15.

Sample Clause A–6:

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

A–7—CONFIDENTIALITY AND SECURITY (ALL INSTITUTIONS)

A bank may use this clause, as applicable, to meet the requirement of § 40.6(a)(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A–7:

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

[65 FR 35196, June 1, 2000. Redesignated and amended at 74 FR 62916, 62925, Dec. 1, 2009]

PART 41—FAIR CREDIT REPORTING

Subpart A—General Provisions

Sec.
41.1 Purpose.
41.2 Examples.
41.3 Definitions.

Subpart B [Reserved]

Subpart C—Affiliate Marketing

41.20 Scope and definitions.
41.21 Affiliate marketing opt-out and exceptions.
41.22 Scope and duration of opt-out.
41.23 Contents of opt-out notice; consolidated and equivalent notices.
41.24 Reasonable opportunity to opt out.
41.25 Reasonable and simple methods of opting out.
41.26 Delivery of opt-out notices.
41.27 Renewal of opt-out.
41.28 Effective date, compliance date, and prospective application.

Subpart D—Medical Information

41.30 Obtaining or using medical information in connection with a determination of eligibility for credit.
41.31 Limits on redisclosure of information.