DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 40

[Docket No. 00–05]

RIN 1557–AB77

FEDERAL RESERVE SYSTEM

12 CFR Part 216

[Docket No. R–1058]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 332

RIN 3064–AC32

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Part 573

[Docket No. 2000–13]

RIN 1550–AB36

Privacy of Consumer Financial Information

AGENCIES: Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; and Office of Thrift Supervision, Treasury.

ACTION: Joint notice of proposed rulemaking.

SUMMARY: The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of Thrift Supervision, (collectively, the Agencies) are requesting comment on proposed privacy rules published pursuant to section 504 of the Gramm-Leach-Bliley Act (the G-L-B Act or Act). Section 504 authorizes the Agencies to issue regulations as may be necessary to implement notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers to nonaffiliated third parties. Pursuant to section 503 of the G-L-B Act, a financial institution must provide its customers with a notice of its privacy policies and practices. Section 502 prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution satisfies various disclosure and opt-out requirements and the consumer has not elected to opt out of the disclosure. These proposed rules implement the requirements outlined above.

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

ADDRESSES: Comments should be directed to: *Office of the Comptroller of the Currency (OCC):* Communications Division, Office of the Comptroller of the Currency, 250 E Street, SW., Washington, DC 20219, Attention: Docket No. 00–05; FAX number (202) 874–5274 or Internet address: regs.comments@occ.treas.gov. Comments may be inspected and photocopied at the same location.

Board of Governors of the Federal Reserve System (Board): Comments, which should refer to Docket No. R–1058, may be mailed to Ms. Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th and C Streets, NW, Washington, DC 20551 or mailed electronically to regs.comments@federalreserve.gov. Comments addressed to Ms. Johnson also may be delivered to the Board's mail room between 8:45 a.m. and 5:15 p.m. and to the security control room outside of those hours. Both the mail room and the security control room are accessible from the courtyard entrance on 20th Street between Constitution Avenue and C Street, NW. Comments may be inspected in Room MP–500 between 9 a.m. and 5 p.m., pursuant to § 261.12, except as provided in § 261.14, of the Board's Rules Regarding the Availability of Information, 12 CFR 261.12 and 261.14.

Federal Deposit Insurance Corporation (FDIC): Send written comments to Robert E. Feldman, Executive Secretary, Attention: Comments/OES, Federal Deposit Insurance Corporation, 550 17th Street, NW., Washington, DC 20429. Comments may be hand delivered to the guard station at the rear of the 17th Street building (located on F Street) on business days between 7 a.m. and 5 p.m. (Fax number (202) 898–3838). Comments may be inspected and photocopied in the FDIC Public Information Center, Room 100, 801 17th Street, NW., Washington, DC 20429, between 9 a.m. and 4:30 p.m. on business days.

Comments may be submitted to the FDIC electronically over the Internet at *www.fdic.gov.* Further information concerning this option may be found below at ''FDIC's New Electronic Public Comment Site.'' Comments also may be mailed electronically to comments@fdic.gov.

Office of Thrift Supervision (OTS): Send comments to Manager, Dissemination Branch, Information Management & Services Division, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552, Attention Docket No. 2000–13. Hand deliver comments to Public Reference Room, 1700 G Street, NW., lower level, from 9:00 A.M. to 5:00 P.M. on business days. Send facsimile transmissions to FAX Number (202) 906–7755 or (202) 906–6956 (if the comment is over 25 pages). Send e-mails to public.info@ots.treas.gov and include your name and telephone number. Interested persons may inspect comments at 1700 G Street, NW., from 9 a.m. until 4 p.m. on business days.

FOR FURTHER INFORMATION CONTACT:

0CC

Amy Friend, Assistant Chief Counsel (202) 874–5200
Mark Tenhundfeld, Assistant Director, Legislative and Regulatory Activities Division (202) 874–5090
Michael Bylsma, Director, Community and Consumer Law (202) 874–5750
Steve Van Meter, Senior Attorney, Community and Consumer Law (202) 874–5750
Karen Furst, Policy Analyst, Economic and Policy Analysis (202) 874–4509
Paul Utterback, National Bank Examiner, Bank Supervision Policy (202) 874–5461, or
Jeffery Abrahamson, Attorney, Legislative and Regulatory Activities Division (202) 874–5090

Board

Oliver I. Ireland, Associate General Counsel (202) 452–3625
Stephanie Martin, Managing Senior Counsel (202) 452–3198, or
Thomas Scanlon, Attorney (202) 452–3594, Legal Division, or
Adrienne D. Hurt, Assistant Director (202) 452–2412
Jane J. Gell, Managing Counsel (202) 452–3667, or
James H. Mann, Attorney (202) 452–2412, Division of Consumer and Community Affairs.
For the hearing impaired only, contact Diane Jenkins, Telecommunications Device for the Deaf (TDD) (202) 452–3544, Board of Governors of the Federal Reserve System, 20th and C Streets, NW, Washington, DC 20551.

FDIC

Deanna Caldwell, Community Affairs Officer, Division of Compliance and Consumer Affairs, (202) 736–0141
James K. Baebel, Senior Review Examiner, Division of Compliance and Consumer Affairs, (202) 736–0229
Robert A. Patrick, Counsel, Regulations and Legislation Section, (202) 898–3757

Marc J. Goldstrom, Counsel, Regulations and Legislation Section, (202) 898–8807
Marilyn E. Anderson, Senior Counsel, Regulations and Legislation Section, (202) 898–3522
Nancy Schucker Recchia, Counsel, Regulations and Legislation Section, (202) 898–8885.

OTS

Christine Harrington, Counsel (Banking and Finance), (202) 906–7957
Paul Robin, Assistant Chief Counsel, (202) 906–6648, Regulations and Legislation Division; or
Cindy Baltierra, Program Analyst, Compliance Policy (202) 906–6540, Office of Thrift Supervision, 1700 G Street, NW., Washington DC 20552.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

I. Background
II. Section-by-Section Analysis
III. FDIC's New Electronic Public Comment Site
IV. Regulatory Analysis
A. Paperwork Reduction Act
B. Regulatory Flexibility Act
C. Executive Order 12866
D. Unfunded Mandates Act of 1995
V. Solicitation of Comments on Use of ''Plain Language''

I. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Pub. L. 106–102, codified at 15 U.S.C. 6801 *et seq.*) into law. Subtitle A of Title V of the Act, captioned Disclosure of Nonpublic Personal Information, limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. Title V also requires the Agencies, the Secretary of the Treasury, the National Credit Union Administration (NCUA), the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC), after consulting with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, to prescribe such regulations as may be necessary to carry out the purposes of the provisions in Title V that govern disclosure of nonpublic personal information.

The Agencies have prepared proposed rules to implement Subtitle A that are consistent and comparable to the extent possible, as is required by the statute.[1] Except where noted in the discussion of the proposed definitions of ''nonpublic personal information,'' ''personally identifiable financial information,'' and ''publicly available information,'' the texts of the Agencies'' proposed regulations are substantively identical. The Agencies request comment on all aspects of the proposed rules as well as comment on the specific provisions and issues highlighted in the section-by-section analysis below.

II. Section-by-Section Analysis

The discussion that follows applies to each of the Agencies' proposed rules. Given that each agency will assign a different part to its privacy rule, the citations are to sections only, leaving citations to part numbers blank.

§ __.1 Purpose and Scope

Proposed paragraph (a) of this section identifies three purposes of the rules. First, the rules require a financial institution to provide notice to consumers about the institution's privacy policies and practices. Second, the rules describe the conditions under which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party. Third, the rules provide a method for a consumer to ''opt out'' of the disclosure of that information to nonaffiliated third parties, subject to the exceptions in proposed §§ __.9,__.10, and__.11, as discussed below.

Proposed paragraph (b) sets out the scope of the banking agencies' rules and tracks the scope of enforcement set out in section 505(a) of the G–L–B Act. This paragraph notes that the rules apply only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes.

The G–L–B Act and the proposed rules apply to domestic offices of United States banks and domestic branches and agencies of foreign banks. The Agencies request comment on whether the rules should apply to foreign financial institutions that solicit business in the United States but that do not have an office in the United States.

§ __.2 Rule of Construction

Proposed § __.2 of the rules sets out a rule of construction intended to clarify the effect of the examples used in the rules. Given the wide variety of transactions that Title V of the G–L–B Act covers, the Agencies propose to adopt rules of general applicability and provide examples of conduct that would, and would not, comply with the rule. While the general rules are consistent among the Agencies' proposals to the extent possible, the examples used by the Federal banking agencies differ on occasion from those used by the other agencies in order to provide guidance that may be most meaningful to entities within a given agency's jurisdiction.

The examples are provided in furtherance of the Federal banking agencies' obligation under section 722 of the G–L–B Act to use ''plain language'' in all proposed and final rules published after January 1, 2000. These examples are not intended to be exhaustive; rather, they are intended to provide guidance about how the rules would apply in specific situations. The Agencies invite comment on whether including examples in the rule is useful and suggestions on additional or different examples that may be helpful in illustrating compliance with the rule.

§ __.3 Definitions

a. *Affiliate.* The proposed rules adopt the definition of ''affiliate'' that is used in section 509(6) of the G–L–B Act. An affiliation will be found when one company ''controls'' (which is defined in § __.3(g), below), is controlled by, or is under common control with another company. The definition includes both financial institutions and entities that are not financial institutions.

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

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

c. *Collect.* The proposed rules define ''collect'' to mean obtaining any information that is organized or retrievable on a personally identifiable

[1] The NCUA, FTC, SEC, and the Treasury Department also have participated in the rulemaking process, and the NCUA, FTC, and SEC will separately issue comparable proposed rules.

basis, irrespective of the source of the underlying information. Several sections of the proposed rule (*see, e.g.,* §§ __.6 and__.7) impose obligations that arise when a financial institution collects information about a consumer. This proposed definition clarifies that these obligations arise when the information enables the user to identify a particular consumer. It also clarifies that the obligations arise regardless of whether the financial institution obtains the information from a consumer or from some other source.

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

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

The G–L–B Act distinguishes ''consumers'' from ''customers'' for purposes of the notice requirements imposed by the Act. As explained more fully in the discussion of proposed § __.4, below, a financial institution is required to give a ''consumer'' the notices required under Title V only if the institution intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party for a purpose that is not authorized by one of several exceptions set out in proposed §§ __.10 and__.11. By contrast, a financial institution must give all ''customers,'' at the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship, a notice of the institution's privacy policy.

A person is a ''consumer'' under the proposed rules if he or she obtains a financial product or service from a financial institution. The definition of ''financial product or service'' in proposed § __.3(k), below, includes, among other things, the evaluation by a financial institution of an application that a person submits to obtain a financial product or service. Thus, a financial institution that intends to share nonpublic personal information about a consumer with nonaffiliated third parties outside of the exceptions described in §§ __.10 and__.11 will have to give the requisite notices, even if the consumer does not enter into a customer relationship with the institution.

The examples that follow the definition of ''consumer'' clarify when someone is a consumer. They include situations where someone applies for a loan or provides information for the purpose of determining whether he or she prequalifies for a loan, a person providing information in connection with seeking to obtain financial advisory services, and a person who negotiates a workout of a loan. The examples also clarify the status of someone whose loan has been sold.

f. *Consumer reporting agency.* The proposed rules adopt the definition of ''consumer reporting agency'' that is used in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)). This term is used in proposed §§ __.11 and__.13.

g. *Control.* The proposed rules define ''control'' using the tests applied in section 23A of the Federal Reserve Act (12 U.S.C. 371c). This definition is used to determine when companies are affiliated (*see* discussion of proposed § __.3(a), above), and would result in financial institutions being considered as affiliates regardless of whether the control is by a company or individual.

h. *Customer.* The proposed rules define ''customer'' as any consumer who has a ''customer relationship'' with a particular financial institution. As is explained more fully in the discussion of proposed § __.4, below, a consumer becomes a customer of a financial institution at the time of entering into a continuing relationship with the institution. Thus, for instance, a consumer would become a customer at the time the consumer executes the documents needed to open a deposit account or borrow money from a financial institution.

The distinction between consumers and customers determines what notices a financial institution must provide. If a consumer never becomes a customer, the institution is not required to provide any notices to the consumer unless the institution intends to disclose nonpublic personal information about that consumer to nonaffiliated third parties outside of the exceptions as set out in §§ __.10 and__.11. By contrast, if a consumer becomes a customer, the institution must provide a copy of its privacy policy prior to the time it establishes the customer relationship and at least annually thereafter during the continuation of the customer relationship.

i. *Customer relationship.* The proposed rules define ''customer relationship'' as a continuing relationship between a consumer and a financial institution whereby the institution provides a financial product or service that is to be used by the consumer primarily for personal, family, or household purposes.[2] Because the G–L–B Act requires annual notices of the financial institution's privacy policies to its customers, the Agencies have interpreted the Act as requiring more than isolated transactions between a bank and a consumer to establish a customer relationship, unless it is reasonable to expect further contact about that transaction between the bank and consumer afterwards. Thus, the proposed rules define ''customer relationship'' as one that generally is of a continuing nature. As noted in the examples that follow the definition, this would include, for instance, maintaining a deposit, loan, trust, or investment account.

A one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. The examples that follow the definition of ''customer relationship'' clarify, for instance, that a purchase of an insurance policy would be sufficient to establish a customer relationship because of the continuing nature of the product, whereas using an automated teller machine (ATM) at a bank at which a consumer transacts no other business, purchasing traveler's checks or money orders, or cashing a check would not. While a person engaging in one of these latter types of transactions would be a consumer under the regulation (thereby requiring the financial institution to provide notices *if* the institution intends to disclose nonpublic personal information about the consumer to nonaffiliated third parties outside of the exceptions), the consumer would not be a customer. A consumer would not necessarily become a customer simply by repeatedly engaging in isolated transactions, such as withdrawing funds at regular intervals from an ATM owned by an institution with whom the consumer has no account.

The examples also clarify that a consumer will have a customer relationship with a financial institution that makes a loan to the consumer and then sells the loan but retains the servicing rights. In that case, the person will be a customer of both the institution that sold the loan and the institution that bought it.

[2] A ''customer'' may be defined differently for purposes of other regulations. *See, e.g.,* 12 CFR 7.4002.

j. *Financial institution.* The proposed rules define ''financial institution'' as any institution the business of which is engaging in activities that are financial in nature, or incidental to such financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). The proposed rules also exempt from the definition of ''financial institution'' those entities specifically excluded by the G–L–B Act.

k. *Financial product or service.* The proposed rules define ''financial product or service'' as a product or service that a financial institution could offer as an activity that is financial in nature, or incidental to such a financial activity, under section 4(k) of the Bank Holding Company Act of 1956, as amended. An activity that is complementary to a financial activity, as described in section 4(k), is not included in the definition of ''financial product or service'' under this part. The proposed rules' definition includes the financial institution's evaluation of information collected in connection with an application by a consumer for a financial product or service even if the application ultimately is rejected or withdrawn. It also includes the distribution of information about a consumer for the purpose of assisting the consumer to obtain a financial product or service.

l. *Government regulator.* The proposed rules adopt the definition of ''government regulator'' that includes each of the Agencies participating in this rulemaking, the Secretary of the Treasury, the NCUA, FTC, SEC, and State insurance authorities under the circumstances identified in the definition. This term is used in the exception set out in proposed § __.11(a)(4) for disclosures to law enforcement agencies, ''including government regulators.''

m. *Nonaffiliated third party.* Paragraph (1) of the proposed definition of ''nonaffiliated third party'' provides that the term means any person (which includes natural persons as well as corporate entities such as corporations, partnerships, trusts, and so on) except: (1) An affiliate of a financial institution, and (2) a joint employee of a financial institution and a third party. This paragraph is intended to be substantively the same as the definition used in section 509(5) of the G–L–B Act. Paragraph (2) of the proposed definition provides that ''nonaffiliated third party'' includes any company that is an affiliate by virtue of the direct or indirect ownership or control of the company by the financial institution or one of its affiliates in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act, whether or not the financial institution is affiliated with a bank or is relying on the authority of those sections.

n. *Nonpublic personal information.* Section 509(4) of the G–L–B Act defines ''nonpublic personal information'' to mean ''personally identifiable financial information'' (which term is not defined in the Act) that is provided by a consumer to a financial institution, results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. Any list, description, or other grouping of consumers—and ''publicly available information'' (which also is undefined in the G–L–B Act) pertaining to them—that is derived using any nonpublic personal information other than publicly available information also is included in the definition of ''nonpublic personal information.''

The proposed rules implement this provision of the G–L–B Act by restating, in paragraph (1) of proposed §__.3(n), the categories of information described above. However, the proposed rules present two alternatives concerning the treatment, for purposes of the definition of ''nonpublic personal information,'' of information that can be obtained from sources available to the general public. The alternatives are based on differences in the definitions of ''personally identifiable financial information'' and ''publicly available information'' which, when read together, result in more information being treated as ''nonpublic personal information'' under Alternative A than would be the case under Alternative B.

Alternative A excludes publicly available information from the scope of ''nonpublic personal information'' only in two circumstances. The first is when the information is part of a list, description, or other grouping of consumers that is derived without using personally identifiable financial information. The second is when information, not provided by a consumer and not resulting from a transaction with the consumer, is otherwise obtained by a financial institution in connection with providing a financial product or service to the consumer. However, in order for the information to be considered ''publicly available'' under Alternative A, the information must be obtained from government records, widely distributed media, or government-mandated disclosures. The fact that the information is available from those sources is immaterial if the financial institution does not actually obtain the information from one of them.

Alternative B [3] similarly excludes publicly available information from the scope of ''nonpublic personal information'' when the information is part of a list, description, or other grouping of consumers that is derived without using personally identifiable financial information. However, Alternative B also excludes any other publicly available information, unless the information is part of a list, description, or other grouping of consumers that is derived using personally identifiable financial information. Under Alternative B, information need only be available from a public source for it to be considered ''publicly available.'' If the information is lawfully available to the general public, then it will be publicly available and excluded from the scope of ''nonpublic personal information'' regardless of whether the institution obtains it from a publicly available source (unless, as previously noted, it is part of a list of consumers that is derived using personally identifiable information). As a result of this approach, the fact that information has been given to a financial institution by a consumer does not automatically extend to that information the protections afforded to nonpublic personal information.

The two alternatives will produce the same results in many instances. Under Alternative A, a person's name, address, and other information that typically is thought of as publicly available is treated as *nonpublic* if that information is provided by the person to a bank in connection with obtaining a financial product or service. Thus, a bank would be unable to disclose such information under Alternative A to a nonaffiliated third party unless the bank complies with the notice and opt out requirements discussed below. Under Alternative B, if the person's name and address were available from public sources, they would be *publicly available* information. However, even under Alternative B, the bank would have to comply with the notice and opt out requirements before sharing that information with nonaffiliated third parties if the information was included on a customer list.

The two alternatives will produce different results, however, in the situation where a bank wants to disclose the name, address, or other information

[3] The Board's proposed rule sets out Alternative B only.

available to the general public about an individual. In that situation, Alternative A would require compliance with the notice and opt out requirements. Alternative B would not, because the information would not be part of a list, description, or other grouping of consumers. The Agencies invite comment on both alternatives.

The Agencies also specifically invite comment on whether either definition of ''nonpublic personal information'' would cover information about a consumer that contains no indicators of a consumer's identity. For instance, if a mortgage lender provided information about its mortgage loans (such as loan-to-value ratios, interest rates, census tracts of mortgaged property, payment history, credit scores, and income) to a nonaffiliated third party for the purpose of preparing market studies, would the lender, without notice or opt out to the consumer, be permitted to do so if the information contains no personal identifiers?

o. *Personally identifiable financial information.* As discussed above, the G–L–B Act defines ''nonpublic personal information'' to include, among other things, ''personally identifiable financial information'' but does not define the latter term.

As a general matter, the proposed rules treat any personally identifiable information as financial if it is obtained by a financial institution in connection with providing a financial product or service to a consumer. The Agencies believe that this approach reasonably interprets the word ''financial'' and creates a workable and clear standard for distinguishing information that is financial from other personal information. The Agencies recognize that this interpretation may result in certain information being covered by the rules that may not be considered intrinsically financial, such as health status, and specifically invite comment on the proposed definition of ''personally identifiable financial information.''

The proposed rules define ''personally identifiable financial information'' to include three categories of information. While these three categories are for the most part identical in both alternatives (see discussion of category 3, below, concerning a difference between the categories), the differences in how Alternatives A and B treat publicly available information result in different applications of what personally identifiable financial information is included within the definition of ''nonpublic personal information.''

The first category of information considered to be ''personally identifiable financial information'' is any information that a consumer provides a financial institution in order to obtain a financial product or service. As noted in the examples that follow the definition, this would include information provided on an application to obtain a loan, credit card, or other financial product or service. If, for instance, medical information is provided on an application to obtain a financial product or service (such as would be the case if a consumer applies for a life insurance policy), that information would be considered ''personally identifiable financial information'' for purposes of the proposed rules.

The second category of information covered by the proposed definition of ''personally identifiable financial information'' includes any information resulting from any transaction between the consumer and the financial institution involving a financial product or service. This would include, as noted in the examples following the definition, account balance information, payment or overdraft history, and credit or debit card purchase information.

The third category includes any financial information about a consumer otherwise obtained by the financial institution in connection with providing a financial product or service to the consumer. This would include, for example, information obtained from a consumer report or from an outside source to verify information a consumer provides on an application to obtain a financial product or service. There is a difference in the statement of the third category between Alternatives A and B. Alternative A expressly excludes from this category publicly available information, while Alternative B does not. However, given the definitions of ''nonpublic personal information'' and ''publicly available information'' in Alternative B, the result is that any of the three categories of personally identifiable information in Alternative B will exclude publicly available information from the personally identifiable financial information that is considered ''nonpublic personal information.''

The examples clarify that the definition of ''personally identifiable financial information'' does not include a list of names and addresses of people who are customers of an entity that is not a financial institution. Thus, the names and addresses of people who subscribe, for instance, to a particular magazine fall outside the definition. If, however, a financial institution includes those names and addresses as part of a list of the institution's customers, then the names and addresses become nonpublic personal information.

The Agencies note that there are other laws that may impose limitations on disclosures of nonpublic personal information in addition to those imposed by the G-L-B Act and these proposed rules. For instance, the Fair Credit Reporting Act imposes conditions on the sharing of application information between affiliates and nonaffiliated third parties. The recently proposed Department of Health and Human Services regulations [4] that implement the Health Insurance Portability and Accountability Act of 1996 would, if adopted in final form, limit the circumstances under which medical information may be disclosed. There may be State laws that affect a financial institution's ability to disclose information. Thus, financial institutions will need to monitor and comply with applicable legislative and regulatory developments that affect the disclosure of consumer information.

The Agencies seek comment on whether further definition of ''personally identifiable financial information'' would be helpful.

p. *Publicly available information.* The proposed rules contain two versions of the definition of ''publicly available information.'' For the most part, the definitions are identical, and differ only in that Alternative A does not treat information as publicly available unless it is obtained from one of the public sources listed in the proposed rules. Alternative B, by contrast, treats information as publicly available if it *could* be obtained from one of the public sources listed in the rules, even if it was obtained from a source not listed in the definition. The Agencies invite comments on which alternative is more appropriate.

The remaining parts of the two alternative versions are identical. Thus, under either alternative, the definition of ''publicly available information'' includes information from official public records, such as real estate recordations or security interest filings. It also includes information from widely distributed media (such as a telephone book, television or radio program, or newspaper) and information that is required to be disclosed to the general public by Federal, State, or local law (such as securities disclosure documents). The proposed rules state that information obtained over the Internet will be considered publicly available information if the information

[4] 64 FR 59918 (Nov. 3, 1999).

is obtainable from a site available to the general public without requiring a password or similar restriction. The Agencies invite comment on what information is appropriately considered publicly available, particularly in the context of information available over the Internet.

q. *You.* For those Agencies that use the pronoun ''you'' to refer to entities within their primary jurisdiction,[5] the definition of this term will vary with each of the Agencies' regulations based upon the financial institutions under their jurisdictions.

§__.4 Initial Notice to Consumers of Privacy Policies and Practices Required

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

Paragraph (a) of proposed §__.4 states the general rule regarding these notices. Pursuant to that paragraph, a financial institution must provide a clear and conspicuous notice (*i.e.,* a notice that is reasonably understandable and designed to call attention to the nature and significance of the information it provides) that accurately reflects the institution's privacy policies and practices. Thus, a financial institution may not fail to maintain the protections that it represents in the notice that it will provide. The Agencies expect that financial institutions will take appropriate measures to adhere to their stated privacy policies and practices.

The proposed rules do not prohibit affiliated institutions from using a common initial, annual, or opt out notice, so long as the notice is delivered in accordance with the rule and is accurate for all recipients. Similarly, the rules do not prohibit an institution from establishing different privacy policies and practices for different categories of consumers, customers, or products, so long as each particular consumer or customer receives a notice that is accurate with respect to him or her.

Notice to customers. The proposed rules require that a financial institution provide an individual a privacy notice prior to the time that it establishes a customer relationship. Thus, the notices may be provided at the same time a financial institution is required to give other notices, such as those required by the Board's regulations implementing the Truth in Lending Act (12 CFR 226.6). This approach is intended to strike a balance between: (1) Ensuring that consumers will receive privacy notices at a meaningful point along the continuum of ''establishing a customer relationship''; and (2) minimizing unnecessary burdens on financial institutions that may result if a financial institution is required to provide a consumer with a series of notices at different times in a transaction. Nothing in the proposed rules is intended to discourage a financial institution from providing an individual with a privacy notice at an earlier point in the relationship if the institution wishes to do so in order to make it easier for the individual to compare its privacy policies and practices with those of other institutions in advance of conducting transactions.

Paragraph (c) of proposed §__.4 identifies the time a customer relationship is established as the point at which a financial institution and a consumer enter into a continuing relationship. The examples that are provided after the statement of the general rule inform the reader that, for customer relationships that are contractual in nature (including, for instance, deposit accounts, loans, or purchases of a nondeposit product), a customer relationship is established upon the execution by the consumer of the contract that is necessary to conduct the transaction in question. In the case of a credit card account, the customer relationship is established when the consumer opens the account. A consumer opens a credit card account when he or she becomes obligated on the account, such as when he or she makes the first purchase, receives the first advance, or becomes obligated for any fee or charges under the account other than an application fee or refundable membership fee. For transactions that may not involve a contract (including, for instance, providing investment advisory services), a customer relationship will be established if the consumer pays or agrees to pay a fee or commission for the service.

Notice to consumers. For consumers who do not establish a customer relationship, the initial notice may be provided at any point before the financial institution discloses nonpublic personal information to nonaffiliated third parties. As provided in paragraph (b) of the proposed rule, if the institution does not intend to disclose the information in question or intends to make only those disclosures that are authorized by one of the exceptions set out in §§__.10 and __.11 of the proposed rule, it is not required to provide the initial notice.

How to provide notice. Paragraph (d) of proposed §__.4 sets out the rules governing how financial institutions must provide the initial notices. The general rule requires that the initial notice be provided so that each recipient can reasonably be expected to receive actual notice. The Agencies invite comment on who should receive a notice in situations where there is more than one party to an account.

The notice may be delivered in writing or, if the consumer agrees, electronically. Oral notices alone are insufficient. In the case of customers, the notice must be given in a way so that the customer may either retain it or access it at a later time. This requirement that the notice be given in a manner permitting access at a later time does not preclude a financial institution from changing its privacy policy. *See* proposed §__.8(c), below. Rather, the rules are intended only to require that a customer be able to access the most recently adopted privacy policy.

Examples of acceptable ways the notice may be delivered include hand-delivering a copy of the notice, mailing a copy to the consumer's last known address, or sending it via electronic mail to a consumer who obtains a financial product or service from the institution electronically. It would not be sufficient to provide only a posted copy of the notice in a lobby. Similarly, it would not be sufficient to provide the initial notice only on a Web page, unless the consumer is required to access that page to obtain the product or service in question. Electronic delivery generally should be in the form of electronic mail so as to ensure that a consumer actually receives the notice. In those circumstances where a consumer is in the process of conducting a transaction over the Internet, electronic delivery also may include posting the notice on a Web page as described above. If a financial institution and consumer orally agree to enter into a contract for a financial product or service over the telephone, the institution may provide the consumer with the option of receiving the initial notice after providing the product or service so as not to delay the transaction. The Agencies invite comment on the regulatory burden of providing the initial notices and on the methods financial institutions anticipate using to provide the notices.

[5] The OCC has used the term ''bank'' instead of ''you'' in its regulation.

The Agencies recognize that in some circumstances a customer does not have a choice as to the institution with which he or she has a customer relationship, such as when an institution purchases the customer's loan in the secondary market. In these situations, it may not be practicable for the institution to provide a notice prior to establishing the customer relationship. The proposed rules provide that if a financial institution purchases a loan or assumes a deposit liability from another financial institution or in the secondary market and the customer does not have a choice about the purchase or assumption, the acquiring financial institution may provide the initial notice within a reasonable time thereafter. The Agencies invite comment on whether there are other similar situations for which an exception is necessary.

The Agencies also recognize that certain consumers may have requested that a financial institution not send statements, notices, or other communications to them, such as in certain private banking relationships. The Agencies request comment on whether and how the rules should address these situations with respect to the notices required by these rules. The Agencies also request comment on whether there are other situations where providing notice by mail is impracticable.

§ __.5 Annual Notice to Customers Required

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

Section 503(a) of the G–L–B Act requires that the annual notices be provided ''during the continuation'' of a customer relationship. To implement this requirement, the proposed rules state that a financial institution is not required to provide annual notices to a customer with whom it no longer has a continuing relationship. The examples that follow this general rule provide guidance on when there no longer is a continuing relationship for purposes of the rules. These include, for instance, deposit accounts that are treated as dormant by a financial institution, loans that are paid in full or charged off, or assets sold without retaining servicing rights.

There will be certain customer relationships (such as obtaining investment advice from a stock broker) that do not present a clear event after which there is no longer a customer relationship. The proposed rules contain an example intended to cover these situations, stating that a relationship will no longer be deemed continuing for purposes of the proposed rules if the financial institution has not communicated with a customer, other than providing an annual privacy policy notice, for a period of 12 consecutive months.

The Agencies invite comment generally on whether the examples provided in proposed § __.5 are adequate and on whether the proposed standard deeming an account relationship to have terminated after 12 months of no communication is appropriate. The Agencies specifically request comment on whether, in the example of dormant accounts, the applicable standard should be the institution's policies or applicable State law. The Agencies also invite comment on the regulatory burden of providing the annual notices and on the methods financial institutions anticipate using to provide the notices.

§ __.6 Information To Be Included in Initial and Annual Notices of Privacy Policies and Practices

Section 503 of the G–L–B Act identifies the items of information that must be included in a financial institution's initial and annual notices. Section 503(a) of the G–L–B Act sets out the general requirement that a financial institution must provide customers with a notice describing the institution's policies and practices with respect to, among other things, disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) of the Act identifies certain elements that must be addressed in that notice.

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

The information to be included is as follows:

1. Categories of Nonpublic Personal Information That a Financial Institution May Collect

Section 503(b)(2) requires a financial institution to inform its customers about the categories of nonpublic personal information that the institution collects. The proposed rules implement this requirement in § __.6(a)(1) and provide an example of how to comply with this requirement that focuses the notice on the source of the information collected. As noted in the example, a financial institution will satisfy this requirement if it categorizes the information according to the sources, such as application information, transaction information, and consumer report information. Financial institutions may provide more detail about the categories of information collected but are not required to do so by the proposed rules.

2. Categories of Nonpublic Personal Information That a Financial Institution May Disclose

Section 503(a)(1) of the G–L–B Act requires the financial institution's initial and annual notice to provide information about the categories of nonpublic personal information that may be disclosed either to affiliates or nonaffiliated third parties.

The proposed rules implement this requirement in proposed § __.6(a)(2). The examples of how to comply with this rule focus on the content of information to be disclosed. As stated in the relevant examples, a financial institution may satisfy this requirement by categorizing information according to source and providing illustrative examples of the content of the information. These categories might include application information (such as assets and income), identifying information (such as name, address, and social security number), transaction information (such as information about account activity, account balances, and purchases), and information from consumer reports (such as credit history).

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

3. Categories of Affiliates and Nonaffiliated Third Parties to Whom a Financial Institution Discloses Nonpublic Personal Information

As previously noted, section 503(a) includes a general requirement that a financial institution provide a notice to its customers of the institution's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) states that the notice required by section 503(a) shall include certain specified items. Among those is the requirement, set out in section 503(b)(1), that a financial institution inform its customers about its policies and practices with respect to disclosing nonpublic personal information to nonaffiliated third parties. The Agencies believe that, when read together, sections 503(a) and 503(b) of the G–L–B Act require a financial institution's notice to address disclosures of nonpublic personal information to both affiliates and nonaffiliated third parties.

The proposed rules implement this requirement in § __.6(a)(3). The example illustrating how a financial institution may comply with the rules states that a financial institution will adequately categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic personal information about consumers if it identifies the types of businesses in which they engage. Types of businesses may be described by general terms, such as financial products or services, if the financial institution provides illustrative examples of the significant lines of businesses of the recipient, such as retail banking, mortgage lending, life insurance, or securities brokerage.

The G–L–B Act does not require a financial institution to list the categories of persons to whom information may be disclosed pursuant to one of the exceptions set out in proposed §§__.10 and __.11. The proposed rules state that a financial institution is required only to inform consumers that it makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the notice. The Agencies invite comment on whether such a notice would be adequate.

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

4. Information About Former Customers

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

The Agencies have concluded that, when read together, sections 503(a)(2) and 503(b)(1)(B) require a financial institution to include in the initial and annual notices the institution's policies and practices with respect to sharing information about former customers with all affiliates and nonaffiliated third parties. This requirement is set out in the proposed rules at § __.6(a)(4). This requirement does not require a financial institution to provide a notice and opportunity to opt out to a former customer before sharing nonpublic personal information about that former customer with an affiliate.

5. Information Disclosed to Service Providers

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

The proposed rules implement these provisions, in § __.6(a)(5), by requiring that, if a financial institution discloses nonpublic personal information to a nonaffiliated third party pursuant to the exception for service providers and joint marketing, the institution is to include in the initial and annual notices a separate description of the categories of information that are disclosed and the categories of third parties providing the services. A financial institution may comply with these requirements by providing the same level of detail in the notice as is required to satisfy the requirements in proposed §§ __.6(a)(2) and (3).

6. Right to Opt Out

As previously noted, sections 503(a)(1) and 503(b)(1) of the G–L–B Act require a financial institution to provide customers with a notice of its privacy policies and practices concerning, among other things, disclosing nonpublic personal information consistent with section 502 of the Act.

The proposed rules implement this requirement, in proposed § __.6(a)(6), by requiring the initial and annual notices to explain the right to opt out of disclosures of nonpublic personal information to nonaffiliated third parties, including the methods available to exercise that right.

7. Disclosures Made Under the Fair Credit Reporting Act (FCRA)

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

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

8. Confidentiality, Security, and Integrity

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

technical, and physical safeguards of customer information).

The proposed rules implement these provisions by requiring a financial institution to include in the initial and annual notices the institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information. The relevant example in the proposed rules states that a financial institution may comply with the requirement as it concerns confidentiality and security if the institution explains matters such as who has access to the information and the circumstances under which the information may be accessed. The information about integrity should focus on the measures the institution takes to protect against reasonably anticipated threats or hazards. The proposed rules do not require a financial institution to provide technical or proprietary information about how it safeguards consumer information.

The Agencies are in the process of preparing the section 501 standards relating to administrative, technical, and physical safeguards, and anticipate having those standards in place at the time of the issuance of the final privacy rules. This will enable financial institutions to develop the initial and annual notices in light of those standards.

§ __.7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.

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

Section __.7 of the proposed rules implements these provisions. Paragraph (a)(1) of § __.7 sets out the criteria that a financial institution must satisfy before disclosing nonpublic personal information to nonaffiliated third parties. As stated in the text of the proposed rules, these criteria apply to direct and indirect disclosures through an affiliate. The Agencies invite comment on how the right to opt out should apply in the case of joint accounts. Should, for instance, a financial institution require all parties to an account to opt out before the opt out becomes effective? If not and only one of the parties opts out, should the opt out apply only to information about the party opting out or should it apply to information about all parties to the account? The Agencies also request comment on how the opt out right should apply to commingled trust accounts, where a trustee manages a single account on behalf of multiple beneficiaries.

Paragraph (a)(2) defines ''opt out'' in a way that incorporates the exceptions to the right to opt out stated in proposed §§ __.9, __.10, and __.11.

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

The requirement that a consumer have a reasonable opportunity to opt out does not mean that a consumer forfeits that right once the opportunity lapses. The consumer always has the right to opt out (as discussed further in proposed §__.8, below). However, if an individual does not exercise that opt out right when first presented with an opportunity, the financial institution would be permitted to disclose nonpublic personal information to nonaffiliated third parties for the period of time necessary to implement the consumer's opt out direction.

Paragraph (b) of proposed §__.7 clarifies that the right to opt out applies regardless of whether a consumer has established a customer relationship with a financial institution. As noted above, all customers are consumers under the proposed rules. Thus, the fact that a consumer establishes a customer relationship with a financial institution does not change the institution's obligations to comply with the requirements of proposed §__.7(a) before sharing nonpublic personal information about that consumer with nonaffiliated third parties. This also applies in the context of a consumer who had a customer relationship with a financial institution but then terminated that relationship. Paragraph (b) also clarifies that the consumer protections afforded by paragraph (a) of proposed §__.7 apply to all nonpublic personal information collected by a financial institution, regardless of when collected. Thus, if a consumer elects to opt out of information sharing with nonaffiliated third parties, that election applies to all nonpublic personal information about that consumer in the financial institution's possession, regardless of when the information is obtained.

Paragraph (c) of proposed §__.7 states that a financial institution may, but is not required to, provide consumers with the option of a partial opt out in addition to the opt out required by this section. This could enable a consumer to limit, for instance, the types of information disclosed to nonaffiliated third parties or the types of recipients of the nonpublic personal information about that consumer. If the partial opt out option is provided, a financial institution must state this option in a way that clearly informs the consumer about the choices available and consequences thereof.

§__.8 Form and Method of Providing Opt Out Notice to Consumers

Paragraph (a) of proposed §__.8 requires that any opt out notice provided by a financial institution pursuant to proposed §__.7 be clear and conspicuous and accurately explain the right to opt out. The notice must inform the consumer that the institution may disclose nonpublic personal information to nonaffiliated third parties, state that the consumer has a right to opt out, and provide the consumer with a reasonable means by which to opt out.

The examples that follow the general rule state that a financial institution will adequately provide notice of the right to opt out if it identifies the categories of information that may be disclosed and the categories of nonaffiliated third parties to whom the information may be disclosed and that the consumer may opt out of those disclosures. A financial institution that plans to disclose only limited types of information or to only a specific type of nonaffiliated third party may provide a correspondingly narrow notice to consumers. However, to minimize the number of opt out notices a financial institution must provide, the institution may wish to

base its notices on current and anticipated information sharing plans. A new opt out notice is not required for disclosures to different types of nonaffiliated third parties or of different types of information, provided that the most recent opt out notice is sufficiently broad to cover the entities or information in question. Nor is a financial institution required to provide subsequent opt out notices when a consumer establishes a new type of customer relationship with that financial institution, unless the institution's opt out policies differ depending on the type of customer relationship.

The examples also suggest several ways in which a financial institution may provide reasonable means to opt out, including check-off boxes, reply forms, and electronic mail addresses. A financial institution does not provide a reasonable means to opt out if the only means provided is for a consumer to write his or her own letter to the institution to exercise the right, although an institution may honor such a letter if received.

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

Paragraph (c) sets out the rules governing a financial institution's obligations in the event the institution changes its disclosure policies. As stated in that paragraph, a financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless the institution first provides a revised notice and new opportunity to opt out. The institution must wait a reasonable period of time before disclosing information according to the terms of the revised notice in order to afford the consumer a reasonable opportunity to opt out. A financial institution must provide the revised notice of its policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under §__.4(c) and §__.8(b), respectively, which require that the notices be given in a manner so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form.

Paragraph (d) states that a consumer has the right to opt out at any time. The Agencies considered whether to include a time limit by which financial institutions must effectuate a consumer's opt out election, but decided that the wide variety of practices of financial institutions made one limit inappropriate. Instead, the Agencies' rules require that disclosures stop as soon as reasonably practicable.

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

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

§ __.9 Exception to Opt Out Requirements for Service Providers and Joint Marketing

Section 502(b) of the G–L–B Act creates an exception to the opt out rules for the disclosure of information to a nonaffiliated third party for use by the third party to perform services for, or functions on behalf of, the financial institution, including the marketing of the financial institution's own products or services or financial products or services offered pursuant to a joint agreement between two or more financial institutions. A consumer will not have the right to opt out of disclosing nonpublic personal information about the consumer to nonaffiliated third parties under these circumstances, if the financial institution satisfies certain requirements.

First, the institution must, as stated in section 502(b), ''fully disclose'' to the consumer that it will provide this information to the nonaffiliated third party before the information is shared. This disclosure should be provided as part of the initial notice that is required by § __.4. The Agencies invite comment on whether the proposed rules appropriately implement the ''fully disclose'' requirement in section 502(b)(2).

Second, the financial institution must enter into a contract with the third party that requires the third party to maintain the confidentiality of the information. This contract should be designed to ensure that the third party: (a) Will maintain the confidentiality of the information at least to the same extent as is required for the financial institution that discloses it; and (b) will use the information solely for the purposes for which the information is disclosed or as otherwise permitted by §§ __.10 and __.11 of the proposed rules. The Agencies invite comment on the application of proposed § __.9(a)(2)(ii) in the context of financial institutions that contract with credit scoring vendors to evaluate borrower creditworthiness. Specifically, would that section prohibit the vendor from also using the consumers' information without the indicators of personal identity to help improve its scoring models?

The G–L–B Act allows the Agencies to impose requirements on the disclosure of information pursuant to the exception for service providers beyond those imposed in the statute. The Agencies have not done so in the proposed rules, but invite comment on whether additional requirements should be imposed, and, if so, what those requirements should address. The Agencies note, for instance, that joint agreements have the potential to create reputation risk and legal risk for a financial institution entering into such an agreement. The Agencies seek comment on whether the rules should require a financial institution to take steps to assure itself that the product being jointly marketed and the other participants in the joint marketing agreement do not present undue risks for the institution. These steps might include, for instance, ensuring that the financial institution's sponsorship of the product or service in question is evident from the marketing of that product or service. The Agencies also invite comments on any other requirements that would be appropriate to protect a consumer's financial privacy, and on whether the rules should provide examples of the types of joint agreements that are covered.

§ __.10 Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions

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

Paragraph (a) of proposed § __.10 sets out those exceptions, making only stylistic changes to the statutory text that are intended to make the exceptions easier to read. Paragraph (b) sets out the definition of ''necessary to effect, administer, or enforce'' that is contained in section 509(7) of the G–L–B Act, making only stylistic changes intended to clarify the definition.

The exceptions set out in proposed § __.10, and the exceptions discussed in proposed § __.11, below, do not affect a financial institution's obligation to provide initial notices of its privacy policies and practices prior to the time it establishes a customer relationship and annual notices thereafter. Those notices must be provided to all customers, even if the institution intends to disclose the nonpublic personal information only pursuant to the exceptions in proposed § __.10.

§ __.11 Other exceptions to notice and opt out requirements.

As noted above, section 502(e) contains several exceptions to the requirements that otherwise would apply to the disclosures of nonpublic personal information to nonaffiliated third parties. Proposed § __.11 sets out those exceptions that are not made in connection with the administration, processing, servicing, and sale of a consumer's account, and makes stylistic changes intended to clarify the exceptions.

One of the exceptions stated in proposed § __.11 is for disclosures made with the consent or at the direction of the consumer, provided the consumer has not revoked the consent. Following the list of exceptions is an example of consent in which a financial institution that has received an application from a consumer for a mortgage loan informs a nonaffiliated insurance company that the consumer has applied for a loan so that the insurance company can contact the person about homeowner's insurance. Consent in such a situation would enable the financial institution to make the disclosure to the third party without first providing the initial notice required by § __.4 or the opt out notice required by § __.7, but the disclosure must not exceed the purposes for which consent was given. The example also states that consent may be revoked by a consumer at any time by the consumer exercising the right to opt out of future disclosures. The Agencies invite comment on whether safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion. Such safeguards might include, for instance, a requirement that consent be written, that it be indicated on a separate signature line in a relevant document or on a distinct Web page, or that it may be effective for only a limited period of time.

§ __.12 Limits on Redisclosure and Reuse of Information

Section __.12 of the proposed rules implements the Act's limitations on redisclosure and reuse of nonpublic personal information about consumers. Section 502(c) of the Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not, directly or indirectly through an affiliate, disclose the information to any person that is not affiliated with either the financial institution or the third party, unless the disclosure would be lawful if made directly by the financial institution. Paragraph (a)(1) sets out the Act's redisclosure limitation as it applies to a financial institution that receives information from another nonaffiliated financial institution. Paragraph (b)(1) mirrors the provisions of paragraph (a)(1), but applies the redisclosure limits to any nonaffiliated third party that receives nonpublic personal information from a financial institution.

The Act appears to place the institution that receives the information into the shoes of the institution that disclosed the information for purposes of determining whether redisclosures by the receiving institution are ''lawful.'' Thus, the Act appears to permit the receiving institution to redisclose the information to: (1) An entity to whom the original transferring institution could disclose the information pursuant to one of the exceptions in §§ __.9, __.10, or ;__.11, or (2) an entity to whom the original transferring institution could have disclosed the information as described under its notice of privacy policies and practices, unless the consumer has exercised the right to opt out of that disclosure. Because a consumer can exercise the right to opt out of a disclosure at any time, the Act may effectively preclude third parties that receive information to which the opt out right applies from redisclosing the information, except pursuant to one of the exceptions in §§ __.9, __.10, or __.11. The Agencies invite comment on whether the rules should require a financial institution that discloses nonpublic personal information to a nonaffiliated third party to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of that information.

Sections 502(b)(2) and 502(e) (as implemented by §§ __.9, __.10, and __.11 of the proposed rules) describe when a financial institution may disclose nonpublic personal information without providing the consumer with the initial privacy notice and an opportunity to opt out, but those exceptions apply only when the information is used for the specific purposes set out in those sections. Paragraph (a)(2) of proposed § __.12 clarifies this limitation on reuse as it applies to financial institutions. Paragraph (a)(2) provides that a financial institution may use nonpublic personal information about a consumer that it receives from a nonaffiliated financial institution in accordance with an exception under §§ __.9, __.10, or __.11 only for the purpose of that exception. Paragraph (b)(2) applies the same limits on reuse to any nonaffiliated third party that receives nonpublic personal information from a financial institution. The Agencies request comment on whether proposed §§ __.12(a)(2) and __.12(b)(2) would restrict a nonaffiliated third party from using information obtained in accordance with the exceptions in §§ __.9, __.10, and __.11 for purposes beyond the scope of those exceptions if the information is not used in a personally identifiable form. This might occur, for example, in the case of a credit scoring vendor using information to improve its scoring models.

The Agencies invite comments on the meaning of the word ''lawful'' as that term is used in section 502(c). The Agencies specifically solicit comment on whether it would be lawful for a nonaffiliated third party to disclose information pursuant to the exception provided in proposed § __.9 of the rules. Under that exception, a financial institution must comply with certain requirements before disclosing information to a nonaffiliated third party. Given that the statute and proposed rules impose those requirements on the financial institution making the initial disclosure, the Agencies invite comment on whether subsequent disclosures by the third party could satisfy the requirement that those disclosures be lawful when the financial institution is not party to the subsequent disclosure.

§ __.13 Limits on Sharing of Account Number Information for Marketing Purposes

Section 502(d) of the G–L–B Act prohibits a financial institution from disclosing, other than to a consumer reporting agency, account numbers or similar form of access number or access code for a credit card account, deposit account, or transaction account of a

consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. Proposed § __.13 applies this statutory prohibition to disclosures made directly or indirectly by a financial institution.

The Agencies note that there is no exception in Title V to the flat prohibition established by section 502(d). The Statement of Managers contained in the Conference Report to S. 900 encourages the Agencies to adopt an exception to section 502(d) to permit disclosures of account numbers in limited instances. It states:

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

Managers' Statement at 18. The Agencies have not proposed an exception to the prohibition of section 502(d) because of the risks associated with third parties' direct access to a consumer's account. The Agencies seek comment on whether an exception to the section 502(d) prohibition that permits third parties access to account numbers is appropriate, the circumstances under which an exception would be appropriate, and how such an exception should be formulated to provide consumers with adequate protection. The Agencies also seek comment on whether a flat prohibition as set out in section 502(d) might unintentionally disrupt certain routine practices, such as the disclosure of account numbers to a service provider who handles the preparation and distribution of monthly checking account statements for a financial institution coupled with a request by the institution that the service provider include literature with the statement about a product. In addition, the Agencies invite comment on whether a consumer ought to be able to consent to the disclosure of his or her account number, notwithstanding the general prohibition in section 502(d) and, if so, what standards should apply. The Agencies also seek comment on whether section 502(d) prohibits the disclosure by a financial institution to a marketing firm of encrypted account numbers if the financial institution does not provide the marketer the key to decrypt the number.

§ __.14 Protection of Fair Credit Reporting Act

Section 506 makes several amendments to the FCRA to vest rulemaking authority in various agencies and to restore the Agencies' regular examination authority. Paragraph (c) of section 506 states that, except for the amendments noted regarding rulemaking authority, nothing in Title V is to be construed to modify, limit, or supersede the operation of the FCRA, and no inference is to be drawn on the basis of the provisions of Title V whether information is transaction or experience information under section 603 of the FCRA.

Proposed § __.14 implements section 506(c) of the G–L–B Act by restating the statute, making only minor stylistic changes intended to make the rule clearer.

§ __.15 Relation to State Laws

Section 507 of the G–L–B Act states, in essence, that Title V does not preempt any State law that provides greater protections than are provided by Title V. Determinations of whether a State law or Title V provides greater protections are to be made by the Federal Trade Commission (FTC) after consultation with the agency that regulates either the party filing a complaint or the financial institution about whom the complaint was filed. Determinations of whether State or Federal law afford greater protections may be initiated by any interested party or on the FTC's own motion.

Proposed § __.15 is substantively identical to section 507, noting that the proposed rules (as opposed to the statute) do not preempt State laws that provide greater protection for consumers than do the rules.

§ __.16 Effective Date; Transition Rule

Section 510 of the G–L–B Act states that, as a general rule, the relevant provisions of Title V take effect 6 months after the date on which rules are required to be prescribed. However, section 510(1) authorizes the Agencies to prescribe a later date in the rules enacted pursuant to section 504.

Proposed § __.16 states, in paragraph (a), an effective date of November 13, 2000. This assumes that a final rule will be adopted within the time frame prescribed by section 504(a)(3). The Agencies intend to provide at least six months following the adoption of a final rule for financial institutions to bring their policies and procedures into compliance with the requirements of the final rule. The Agencies invite comment on whether six months following adoption of final rules is sufficient to enable financial institutions to comply with the rules.

Paragraph (b) of proposed § __.16 provides a transition rule for consumers who were customers as of the effective date of the rules. Since those customer relationships already will have been established as of the rules' effective date (thereby making it inappropriate to require a financial institution to provide those customers with a copy of the institution's initial notice at the time of establishing a customer relationship), the rules require instead that the initial notice be provided within 30 days of the effective date. The Agencies invite comment on whether 30 days is enough time to permit a financial institution to deliver the required notices, bearing in mind that the G–L–B Act contemplates at least a six-month delayed effective date from the date the rules are adopted.

If a financial institution intends to disclose nonpublic personal information about someone who was a consumer before the effective date, the institution must provide the notices required by §§ __.4 and __.7 and provide a reasonable opportunity to opt out before the effective date. If, in this instance, the institution already is disclosing information about such a consumer, it may continue to do so without interruption until the consumer opts out, in which case the institution must stop disclosing nonpublic personal information about that consumer to nonaffiliated third parties as soon as reasonably practicable.

III. FDIC's New Electronic Public Comment Site

The FDIC has developed a new page on its web site to facilitate the submission of electronic comments in response to this general solicitation (the EPC site). The EPC site provides an alternative to the written letter and may be a more convenient way for you to submit your comments. Commenting through the EPC site will assist the FDIC to more accurately and efficiently analyze comments submitted electronically. If you submit your comments through the EPC site your comments will receive the same consideration that they would receive if submitted in hard copy to the FDIC's street address. Information provided through the EPC site will be used by the FDIC only to assist in its analysis of the proposed regulation. The FDIC will not use an individual's name or any other personal identifier of an individual to retrieve records or information

submitted through the EPC site. Like comments submitted in hard copy to the FDIC's street address, EPC site comments will be made available in their entirety (including the commenter's name and address if the commenter chooses to provide them) for public inspection.

The EPC site will be available on the FDIC's home page at http://www.fdic.gov. You will be able to provide general comments or comments on any specific sections of, or questions on, the proposed rule. You will also be able to view the regulation and Supplementary Information sections that relate to your comments directly on the site. Once you have finished commenting on the sections of interest to you, you may indicate your general approval or disapproval of the proposed regulation by answering the following question: Does the proposed regulation appropriately implement the G–L–B Act to provide the full extent of privacy protections intended by the Act? [Yes/No].

If you choose to answer this question, your response will be used in the FDIC's analysis of public comment on the regulation. The FDIC encourages you to provide written comments in the spaces provided in addition to responding to this specific question. Written comments enable the FDIC to thoughtfully consider possible changes to the proposed regulation.

The FDIC is also interested in your feedback on the EPC site. We have provided a space for you to comment on the site itself. Answers to this question will help the FDIC evaluate the EPC site for use in future rulemaking.

At the conclusion of the EPC site you will have an opportunity to provide us with your name, indicate whether you are an individual, bank, trade association, or government agency, and provide the name of the organization you represent, if applicable. Whether you choose to respond to these questions is entirely up to you. Any responses received may help the FDIC to better understand the public comments it receives.

IV. Regulatory Analysis

A. Paperwork Reduction Act

The Agencies invite comment on:

(1) Whether the collections of information contained in this notice of proposed rulemaking are necessary for the proper performance of each Agency's functions, including whether the information has practical utility;

(2) The accuracy of each Agency's estimate of the burden of the proposed information collections;

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

(4) Ways to minimize the burden of the information collections on respondents, including the use of automated collection techniques or other forms of information technology; and

(5) Estimates of capital or start-up costs and costs of operation, maintenance, and purchases of services to provide information.

Recordkeepers are not required to respond to these collections of information unless they display a currently valid Office of Management and Budget (OMB) control number. The agencies are currently requesting their respective control numbers for these information collections from OMB.

This proposed regulation contains several disclosure requirements. The respondents must prepare and provide the initial notice to all current customers and all new customers at the time of establishing a customer relationship (proposed § __.4(a)). Subsequently, an annual notice must be provided to all customers at least once during a twelve-month period during the continuation of the customer relationship (proposed § __.5(a)). The opt out notice (and partial opt out notice, if applicable; *see* proposed § __.7(a)(1)(iii)) must be provided prior to disclosing nonpublic personal information to certain nonaffiliated third parties. If a financial institution wishes to disclose information in a way that is inconsistent with the notices previously given to a consumer, the institution must provide consumers with revised notices (proposed § __.8(c)).

The proposed regulation also contains consumer reporting requirements. In order for consumers to opt out, they must respond to the institution's opt out notice (proposed §§ __.7(a)(2), (a)(3)(i), and (c)). At any time during their continued relationship with the institution, consumers have the right to change or update their opt out status with the institution (proposed §§ __.8(d) and (e)). The Agencies request public comment on all aspects of the collections of information contained in this proposed rule, including consumer responses to the opt-out notice and consumer changes to their opt-out status with an institution. In light of the uncertainty regarding what institutions will do to comply with the opt-out requirements and how consumers will react, the Agencies estimate a nominal burden stemming from consumer responses of one hour per institution, and will revisit this estimate in light of the comments received.

OCC: The collection of information requirements contained in this notice of proposed rulemaking have been submitted to the Office of Management and Budget for review in accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)). Comments on the collections of information should be sent to the Office of Management and Budget, Paperwork Reduction Project (1557—to be assigned), Washington, DC 20503, with copies to the Legislative and Regulatory Activities Division (1557—to be assigned), Office of the Comptroller of the Currency, 250 E Street, SW, Washington, DC 20219.

The likely respondents are national banks, District of Columbia banks, and Federal branches and agencies of foreign banks.

Estimated average annual burden hours per bank respondent: 45.

Estimated number of bank respondents: 2,400.

Estimated total annual reporting burden: 108,000 hours.

Board: In accordance with section 3506 of the Paperwork Reduction Act of 1995 (44 U.S.C. Ch. 35; 5 CFR 1320, appendix A.1), the Board reviewed the notice of proposed rulemaking under the authority delegated to the Board by the OMB. Comments on the collections of information should be sent to Mary M. West, Chief, Financial Reports Section, Division of Research and Statistics, Mail Stop 97, Board of Governors of the Federal Reserve System, Washington, DC 20551, with a copy to the Office of Management and Budget, Paperwork Reduction Project (7100—to be assigned), Washington, DC 20503.

The likely respondents are state member banks, bank holding companies, affiliates and certain non-bank subsidiaries of bank holding companies, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and agreement corporations.

Estimated number of respondents: 9500.

Estimated average annual burden hours per respondent: 45 hours.

Estimated total annual reporting and disclosure burden: 427,500.

FDIC: The collections of information contained in the notice of proposed rulemaking will be submitted to the OMB in accordance with the Paperwork Reduction Act of 1995. 44 U.S.C. 3507. The FDIC will use any comments received to develop its new burden estimates. Comments on the collections

of information should be sent to Steven F. Hanft, Office of the Executive Secretary, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, DC 20429, with a copy to the Office of Management and Budget, Paperwork Reduction Project (3064—to be assigned), Washington, DC 20503.

The likely respondents are insured nonmember banks.

Estimated number of respondents: 5,764.

Estimated average annual burden hours per respondent: 45 hours.

Estimated total annual reporting and disclosure burden: 259,380 hours.

OTS: The collection of information requirements contained in the notice of proposed rulemaking will be submitted to the OMB in accordance with the Paperwork Reduction Act of 1995. 44 U.S.C. 3507. The OTS will use any comments received to develop its new burden estimates. Comments on the collection of information should be sent to the Dissemination Branch (1550–AB36), Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552, with a copy to the Office of Management and Budget, Paperwork Reduction Project (1550–AB36), Washington, DC 20503.

The likely respondents are savings associations.

Estimated number of respondents: 1,104.

Estimated average annual burden hours per respondent: 45 hours.

Estimated total annual disclosure and recordkeeping burden: 49,680 hours.

B. Regulatory Flexibility Act

OCC: Under the Regulatory Flexibility Act (RFA), the OCC must either provide an Initial Regulatory Flexibility Analysis (IRFA) with a proposed rule or certify that the proposed rule would not have a significant economic impact on a substantial number of small entities. The OCC has decided to publish the following analysis and invites the public's comments on the propose rule's impact on small entities (*i.e.*, for purposes of RFA, small entities include banks with less than $100 million in assets).

A. Reasons for and Objectives of the Proposed Rule; Legal Basis for Rule

The proposed rule implements provisions of Title V, Subtitle A of the G–L–B Act addressing consumer privacy. In general, these statutory provisions require banks to provide notice to consumers about an institution's privacy policies and practices, restrict the ability of a bank to share nonpublic personal information about consumers to nonaffiliated third parties, and permit consumers to prevent the institution from disclosing nonpublic personal information about them to certain non-affiliated third parties by ''opting out'' of that disclosure.

The notice and opt out requirements are imposed by Title V, Subtitle A of the G–L–B Act, and are to become effective within one year from the date the Act was signed into law. Section 504 of the G–L–B Act authorizes the OCC to prescribe ''such regulations as may be necessary'' to carry out the purposes of Title V, Subtitle A. The OCC believes that a regulatory promulgation gives the private sector greater certainty on how to comply with the statute and clearer guidance regarding how it will be enforced.

B. Requirements of the Proposed Rule; Description of Small Entities to Whom Rule Would Apply

Subject to certain exceptions explained below, the proposed rule generally requires that a bank provide all of its *customers* the following notices: (1) An initial privacy notice (prior to the time the customer relationship is established or, for existing customers, within 30 days of the rule's effective date); (2) an opt out notice (prior to the disclosing of the individual's nonpublic personal information to nonaffiliated third parties); and (3) an annual privacy notice for the duration of the customer relationship. A bank's ''customer'' is a consumer with whom the bank has a ''continuing relationship'' (*e.g.*, an ongoing deposit or loan relationship—but does not include a transient relationship, such as the mere purchase of traveler's checks from the bank).

The proposed rule also requires a bank to provide its *consumers* an initial privacy notice and an opt out notice prior to disclosing the individual's nonpublic personal information with nonaffiliated third parties. If the bank does not intend to share such information about its consumers, then no privacy or opt out notice need be given. A bank's ''consumer,'' which is a broader concept than ''customer,'' includes: (1) Individuals who have applied to the bank for a financial service or product; and (2) individuals who have purchased a product or service that results in a transient (as opposed to continuing) relationship (*e.g.*, mere purchase of traveler's checks from a bank).

There are a host of exceptions to the general rules stated above. A bank may share a consumer's nonpublic personal information with nonaffiliated third parties without having to give a privacy and opt out notice if, for example, such sharing is necessary: (1) To effect, administer, or enforce a transaction requested or authorized by the consumer; (2) to protect the security of records pertaining to the consumer, service, product, or transaction; (3) to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability; or (4) to provide information to rating agencies or the bank's attorneys, auditors, and accountants. Also, in cases where a bank enters into a contract with a nonaffiliated third party to undertake joint marketing or to have the third party perform certain functions on behalf of the bank, no opt out notice must be given. In such an instance, the bank must disclose to the consumer that it is providing the information and enter into a contract with the third party that restricts the third party's use of the information and requires the third party to maintain confidentiality of the information.

Because the relevant statute did not provide a general exception for small banks, the proposed rule would apply to all banks, regardless of size, including those with assets of $100 million or less. As of September 30, 1999, 1213 (of 2,383 total) national banks had assets of $100 million or less.

Compliance requirements will vary depending, for example, upon a bank's information sharing practices, whether the bank already has or discloses a privacy policy, and whether the bank already has an opt-out mechanism in place pursuant to the Fair Credit Reporting Act.

As part of the requirement to provide a privacy notice, a bank's practices regarding its collection, sharing, and safeguarding of certain nonpublic personal information must be summarized in writing in a form that is required or permitted by the proposed regulation. However, if the bank does not share such information (or shares only to the extent permitted under the exceptions), its privacy notice may be streamlined. Various surveys suggest that a majority of banks already have privacy policies in place as part of usual and customary business practices. For these institutions, the costs for translating that policy into a notice format should be minimal.

Further, to minimize the burden and costs of distributing privacy policies, the proposed regulation allows each bank to choose the method by which it will distribute required notices. For example, banks may include an annual privacy notice with periodic account statements that the bank already sends to the customer. Also, the initial privacy

notice may be provided with other already-required disclosure statements, such as those required under the Truth in Lending Act.

The OCC believes that the burden imposed by the opt out requirement will be minimized to the extent that a bank must give opt out notices under the FCRA. Under the FCRA, a bank must have an opt out mechanism in place if the bank: (1) Shares certain consumer information (*i.e.*, application or credit report information) with its affiliates, and (2) does not want to be treated as a consumer reporting agency (as will usually be the case). For a bank that gives FCRA notices and that wants to share nonpublic personal information with nonaffiliated third parties, the bank should be able to adapt its existing opt out mechanism to accommodate the requirements of the proposed rule. Of course, a bank need not provide any opt-out notices or set up any opt-out mechanism if it will only be sharing nonpublic information with nonaffiliated third parties to the extent permitted by one of the many exceptions permitted in the proposed rule.

Professional skills needed to comply with the proposed rule may include clerical, computer systems, personnel training, as well as legal drafting and advice. The information collection requirements imposed by the G–L–B Act and the proposed rule are further addressed in the section titled, ''Paperwork Reduction Act.''

C. Relevant Federal Rules Which May Duplicate, Overlap or Conflict With the Proposed Rule

While the scope of the proposed regulation (pursuant to the G–L–B Act) is unique, there may be some overlap in certain circumstances with the following: As noted above, the Fair Credit Reporting Act requires a bank that: (1) Does not want to be treated as a consumer reporting agency; and (2) desires to share certain consumer information (*i.e.*, application or credit report information) with its affiliates, to provide the consumer with a clear and conspicuous notice and an opportunity to opt out of such information sharing. Also, at the time a consumer contracts for an electronic fund transfer service, the Electronic Funds Transfer Act requires the terms and conditions of such transfer to be disclosed, including under what circumstances the bank will in the ordinary course of business disclose information concerning the consumer's account to third persons. The recently proposed Department of Health and Human Services regulations [6] that implement the Health Insurance Portability and Accountability Act of 1996 would, if adopted in final form, limit the circumstances under which medical information may be disclosed. Finally, the Children's Online Privacy Protection Act (under which the Federal banking agencies are charged with enforcement of implementing regulations promulgated by the Federal Trade Commission) generally requires online service operators collecting personal information from a child to obtain parental consent and post a privacy notice on the web site. The OCC seeks comment on additional Federal rules that may duplicate, overlap, or conflict with the proposal.

D. Significant Alternatives to the Proposed Rule That Minimize the Impact on Small Entities

As previously noted, the proposed rule's requirements are expressly mandated by the G–L–B Act. The proposed rule attempts to clarify, consolidate, and simplify the statutory requirements for all covered entities, including small entities. The proposed rule also provides substantial flexibility so that any bank, regardless of size, may tailor its practices to its individual needs. While the OCC may grant exceptions to the opt out requirements set out in sections 502 (a) through (d), section 504(b) of the G–L–B Act requires such exceptions to be ''consistent with the purposes of this subtitle [*i.e.*, Subtitle A of Title V].'' As stated in section 501(a) of the Act, ''It is the policy of the Congress that *each* financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.'' (Emphasis added.) The OCC believes that an exception that would create different levels of protections for consumers based on the size of the institution with whom they conduct business would not be consistent with the purposes of Subtitle A. The OCC welcomes comment on any significant alternatives, consistent with the G–L–B Act, that would minimize the impact on small entities.

Board: The Regulatory Flexibility Act (5 U.S.C. 603) requires an agency to publish an initial regulatory flexibility analysis with any notice of proposed rulemaking. A description of the reasons why action by the agency is being considered and a statement of the objectives of, and legal basis for, the proposed rule, are contained in the supplementary material above. The Board's proposed rule will apply to the following institutions (numbers approximate):

Type of institution	Approx. No.
State member banks	1,000
Bank holding companies	5,900
Bank holding company subsidiaries	2,100
U.S. branches and agencies of foreign banks	400
Edge/Agreement corporations, commercial lending companies	100
Total	9,500

The Board estimates that over 4,500 of the respondents could be considered small institutions with assets less than $100 million.

Overlap with other Federal rules. While the scope of the proposed regulation (pursuant to the G–L–B Act) is unique, it may, in certain circumstances, overlap with the following statutes and regulations:

1. The Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)) requires a bank that: (1) Does not want to be treated as a consumer reporting agency; and (2) desires to share certain consumer information (that is, application or credit report information) with its affiliates, to provide the consumer with a clear and conspicuous notice and an opportunity to opt out of such information sharing.

2. At the time a consumer contracts for an electronic fund transfer service, the Electronic Funds Transfer Act (15 U.S.C. 1693c(a)(9)) requires the terms and conditions of such transfer to be disclosed, including under what circumstances the bank will in the ordinary course of business disclose information concerning the consumer's account to third persons.

3. The recently proposed Department of Health and Human Services regulations [7] that implement the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 3120d–1 *et seq.*) would, if adopted in final form, limit the circumstances under which medical information may be disclosed.

4. The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6502) (under which the Federal banking agencies are charged with enforcement of implementing regulations promulgated by the Federal Trade Commission) generally requires online service operators collecting personal information from a child to obtain

[6] 64 FR 59918 (Nov. 3, 1999).

[7] 64 FR 59918 (Nov. 3, 1999).

parental consent and post a privacy notice on the web site.

New compliance requirements. The proposed rule contains new compliance requirements for all covered institutions, most of which are required by the G–L–B Act. The institutions will be required to prepare notices of their privacy policies and practices and provide those notices to consumers as specified in the rule. Institutions that disclose nonpublic personal information about consumers to nonaffiliated third parties will be required to provide opt out notices to consumers as well as a reasonable opportunity to opt out of certain disclosures. These institutions will have to develop systems for keeping track of consumers' opt out directions. Some institutions, particularly those that disclose nonpublic information about consumers to nonaffiliated third parties, will likely need the advice of legal counsel to ensure that they comply with the rule, and may also require computer programming changes and additional staff training. The Board does not have a practicable or reliable basis for quantifying the costs of the proposed rule or any alternatives, but seeks comment on the potential costs.

Exemptions for small institutions. The Board believes the requirements of the Act and this rule will create additional burden for covered institutions, particularly those that disclose nonpublic personal information about consumers to nonaffiliated third parties. The rule applies to all covered institutions, regardless of size. The Act does not provide the Board with the authority to exempt a small institution from the requirement to provide a notice of its privacy policies and practices to a consumer with whom it establishes a customer relationship. Although the Board could exempt small institutions from providing a notice and opportunity for consumers to opt out of certain information disclosures, the Board does not believe that such an exemption would be appropriate, given the purpose of the Act to protect the confidentiality and security of nonpublic personal information about consumers. The Board believes that the burden is relatively small for institutions that do not disclose nonpublic personal information about consumers to nonaffiliated third parties. These institutions may provide relatively simple initial and annual notices to consumers with whom they establish customer relationships.

The Board recognizes that the Congressional Conferees on the Act wished to ensure that smaller financial institutions are not placed at a competitive disadvantage by a statutory regime that permits certain information to be shared freely within an affiliate structure while limiting the ability to share that same information with nonaffiliated third parties. The Conferees stated that, in prescribing regulations, the federal regulatory agencies should take into consideration any adverse competitive effects upon small commercial banks, thrifts, and credit unions.[8] At this time, it is not clear the extent to which small institutions will be placed at a disadvantage by information-sharing among affiliates in large institutional families. The Board believes that further experience under the regulation would be appropriate before considering any exemptions in this area for small institutions.

The Board requests comment on the burdens associated with the proposed rule and whether any exemptions for small institutions would be appropriate.

FDIC: The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires an agency to publish an initial regulatory flexibility analysis with this proposed rule, except to the extent provided in the RFA, whenever the agency is required to publish a general notice of proposed rulemaking for a proposed rule. The FDIC cannot at this time determine whether the proposed rule would have a significant economic impact on a substantial number of small entities as defined by the RFA.[9] Therefore, pursuant to subsections 603 (b) and (c) of the RFA, the FDIC provides the following initial regulatory flexibility analysis.

Reasons for Proposed Rule

The FDIC is requesting comment on proposed privacy rules published pursuant to section 504 of the G–L–B Act. Section 504 requires the Agencies in consultation with representatives of State insurance authorities to issue regulations implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers to nonaffiliated third parties. These requirements are expressly mandated by the G–L–B Act. It is the view of the FDIC that the G–L–B Act's requirements account for most, if not, all of the economic impact of the proposed rule.

Statement of Objectives and Legal Basis

The **SUPPLEMENTARY INFORMATION** section above contains this information. The legal basis for the proposed rule is the G–L–B Act.

Description/Estimate of the Small Entities to Which the Rule Applies

The proposed rule would apply to all FDIC-insured State nonmember banks, approximately 3,700 of which are small entities as defined by the RFA.

Projected Reporting, Recordkeeping and Other Compliance Requirements

The information collection requirements imposed by G–L–B Act and the proposed rule are discussed above in the section titled, ''Paperwork Reduction Act.''

General Requirements

Pursuant to section 503 of the G–L–B Act and §§ 332.4—332.6 of the regulation, a financial institution must provide its customers with a notice of its privacy policies and practices. Section 502 of the G–L–B Act and §§ 332.7–332.12 of the regulation prohibit a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution satisfies various disclosure requirements and the consumer has elected not to opt out of the disclosure.

The statute and proposed rule require a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and non-affiliated third parties. Institutions are required to provide this notice at the time of establishing a customer relationship and annually thereafter. Recent experience has shown that it is a usual and customary business practice of financial institutions. KPMG reported in a recent industry survey of large and small banks that 71% of bankers said their institutions already had privacy policies in place either company-wide or in some selected units.[10] Another recent survey of Internet banking sites conducted by federal banking regulators concluded that over 62% of financial institutions that collected personal information online provided a privacy policy or information practice statement.[11] Furthermore, a number of industry groups have developed model privacy policies that are available as part of their

[8] H. R. Conf. Rep. No. 106–434, at 173 (1999).

[9] The RFA defines the term ''small entity'' in 5 U.S.C. 601 by reference to definitions published by the Small Business Administration (SBA). The SBA has defined a ''small entity for banking purposes as a national or commercial bank, savings institution or credit union with less than $100 million in assets.'' *See* 13 CFR 121.201.

[10] ''KPMG Analysis Consumer Privacy Policies: Write Now.'' Online *Reuters* 19 Jan. 2000.

[11] ''Interagency Financial Institution Web Site Privacy Survey Report.'' *FDIC Press Release* 9 November 1999.

self-regulatory efforts in the privacy area.[12] The FDIC believes the establishment of a privacy policy is a usual and customary business practice and the costs for translating that policy into a disclosure format should be minimal. The FDIC seeks any information or comment on the costs for creating privacy policy disclosures.

To minimize the burden and costs to financial institutions of distributing privacy policies, the proposed regulation allows each bank to choose the method by which it will distribute required disclosure statements. Institutions may provide customers with a privacy disclosure statement with periodic statements, with other required disclosure statements, via electronic mail to consumers who obtain a financial product or service electronically, and other acceptable means described in the proposed regulation. The FDIC believes that the cost of distributing privacy disclosure statements will be minimal and seeks any information or comment on the costs for distributing privacy policy disclosures.

The statute and proposed rule describe the conditions under which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party. A number of exceptions are provided for nonaffiliated third parties performing services for the institution. The rules require institutions to develop a method to allow customers to opt out of non-affiliated third party information sharing. Only those institutions that intend to share nonpublic personal information with third parties outside of the exemptions provided are required to establish ''opt out'' disclosure and processing procedures. Furthermore, only those institutions that share nonpublic personal information with third parties outside of the exemptions provided could be expected to encounter any reduction in revenue as a result of the diminished value of information sales. The FDIC informally surveyed its regional offices to determine the costs of implementing the opt out provisions of the proposed regulation. Based on the observations by FDIC examiners, the FDIC believes that the costs to implement opt out provisions of the regulation for small insured nonmember banks will be minimal. Few nonaffiliated third party information sharing arrangements could be identified that would fall outside the exceptions provided in the regulation. Congress recognized the lack of information available on affiliate information sharing practices by requiring the regulators to conduct a ''Study of Information Sharing Among Financial Affiliates'' that focuses on the practice of institutions sharing confidential customer information with affiliates and non-affiliated third parties. This study is due subsequent to release of this regulation. The FDIC seeks further comment on the information sharing practices and actual costs of implementing the opt out disclosure and processing requirements of the proposed regulation.

Identification of Duplicative, Overlapping, or Conflicting Federal Rules

While the scope of the proposed regulation (pursuant to the G–L–B Act) is unique, there may be some overlap in certain circumstances with the following: As noted above, the FCRA requires a bank that: (1) Does not want to be treated as a consumer reporting agency; and (2) desires to share certain consumer information (*i.e.,* application or credit report information) with its affiliates, to provide the consumer with a clear and conspicuous notice and an opportunity to opt out of such information sharing. Also, at the time a consumer contracts for an electronic fund transfer service, the Electronic Funds Transfer Act requires the terms and conditions of such transfer to be disclosed, including under what circumstances the bank will in the ordinary course of business disclose information concerning the consumer's account to third persons. Finally, the Children's Online Privacy Protection Act (under which the Federal banking agencies are charged with enforcement of implementing regulations promulgated by the Federal Trade Commission) generally requires online service operators collecting personal information from a child to obtain parental consent and post a privacy notice on the web site. The FDIC seeks comments and information about any such rules, as well as any other state, local, or industry rules or policies that require financial institutions to implement business practices that would comply with the requirements of the proposed rule.

Discussion of Significant Alternatives

As previously noted, the proposed rule's requirements are expressly mandated by the G–L–B Act. The proposed rule attempts to clarify, consolidate, and simplify the statutory requirements for all covered entities, including small entities. The proposed rule also provides substantial flexibility so that any bank, regardless of size, may tailor its practices to its individual needs. While the FDIC may grant exceptions to the opt out requirements set out in sections 502(a) through (d), section 504(b) of the G–L–B Act requires such exceptions to be ''consistent with the purposes of this subtitle [*i.e.,* Subtitle A of Title V].'' As stated in section 501(a) of the Act, ''It is the policy of the Congress that *each* financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.'' (Emphasis added.) The FDIC believes that an exception that would create different levels of protections for consumers based on the size of the institution with whom they conduct business would not be consistent with the purposes of Subtitle A. The FDIC welcomes comment on any significant alternatives, consistent with the G–L–B Act, that would minimize the impact on small entities.

OTS: The Regulatory Flexibility Act requires federal agencies to either prepare an initial regulatory flexibility analysis (IRFA) with this proposed rule or certify that the proposed rule would not have a significant economic impact on a substantial number of small entities.[13] The OTS cannot, at this time, determine whether the proposed rule would have a significant economic impact on a substantial number of small institutions. Therefore, OTS includes the following IRFA.

A description of the reasons why OTS is considering this action, and a statement of the objectives of, and legal basis for, the proposed rule are in the supplementary material above.

A. Small Entities to Which the Proposed Rule Would Apply

The proposed rule would apply to all financial institutions, without regard to the institutions' size. Small depository institutions are generally defined, for Regulatory Flexibility Act purposes, as those with assets under $100 million.[14] This proposed rule would apply to approximately 500 small savings associations.

B. Requirements of the Proposed Rule

As described more fully above, the proposed rule contains new compliance requirements for all savings associations. Most of the requirements are mandated by the G–L–B Act. Savings associations will be required to prepare

[12] ''Banks Should Tell Customers of Policies to Protect Privacy, Banking Groups Say.'' Online *BNA Electronic Commerce & Law* 16 September 1998.

[13] 5 U.S.C. 605(b).

[14] 13 CFR 121.201, Division H (1999).

notices of their privacy policies and practices and provide those notices to consumers. Savings associations that disclose nonpublic personal information about consumers to nonaffiliated third parties will be required to provide opt out notices to consumers as well as a reasonable opportunity to opt out of certain disclosures. These savings associations will have to develop systems for keeping track of consumers' opt out directions.

C. Reporting, Recordkeeping, and Other Compliance Requirements

The proposed rule would require savings associations to disclose their privacy policies to consumers, and to keep track of any opt out notices the consumers submit.

Many financial institutions may already have established privacy policies and practices and may already be partly or fully prepared to meet the requirements of this proposed rule. Additionally, OTS anticipates that trade associations and others will prepare compliance materials and guidance that financial institutions can use to meet the requirements of this proposed rule.

To the extent that existing practices and available resources are insufficient, financial institutions would need professional skills to comply with this proposed rule. To prepare the required privacy disclosures and opt out notices, financial institutions may need legal or other professional advice and drafting. This would be true for the initial disclosures and notices, and for any subsequent changes to those documents. For financial institutions that publish privacy notices electronically or accept electronic opt outs, computer expertise would be necessary to convert the documents to the appropriate electronic form.

The proposed regulation would allow financial institutions to share consumers' nonpublic personal information with a nonaffiliated third party to perform services for the financial institution. However, § 573.9(a)(2) of the regulation would require institutions in that event to contractually require the third party recipient to maintain the privacy of shared information. In these cases, financial institutions may require legal advice and drafting to ensure that their contracts meet the requirements of the proposed rule.

Financial institutions may further need professional skills to process opt out notices that consumers submit. Some financial institutions may use clerical or computer programmer skills to perform these tasks. Some degree of personnel training may be necessary, such as to train staff on the procedures for entering opt out data into a computer database.

OTS does not have a practicable or reliable basis for quantifying the costs of this proposed rule, or of any alternative to the rule. OTS cannot predict how savings associations would comply with the proposed notice requirements, or how many opt out notices savings associations would receive and need to process. Some savings associations may currently derive revenue from selling information about their customers, and this rule may decrease the amount of that revenue. OTS has no reliable basis for determining the amount of this decrease in revenue at savings associations. The costs of this proposed rule or any alternative to the rule are unpredictable for two reasons. First, Congress has required this regulation to be finalized within six months after G–L–B's enactment. This short time period makes it difficult to survey savings associations or trade organizations for reliable information. Second, and more importantly, the G–L–B Act and this rulemaking are so new that the industry has not had enough time to learn what the law requires and decide how to proceed. Rather than merely guess at the regulatory burden of this proposed rule, OTS solicits comment on the burden and on ways to minimize it, consistent with the G–L–B Act.

D. Significant Alternatives

The requirements in the proposed rule parallel those in the G–L–B Act. The proposed regulation would clarify the statutory requirements in certain areas, and would restate the requirements in a more understandable manner, but would not impose any substantially different requirements.

Congress has decided that ''each'' financial institution must protect consumers' privacy, without regard to the size of the financial institutions with which consumers interact. [15] OTS believes it does not have authority to exempt small entities from Subtitle V of the G–L–B Act.

Although OTS could exempt small savings associations from providing a notice and opportunity for consumers to opt out of certain information disclosures, OTS does not believe that such an exemption would be appropriate, given the purpose of the G–L–B Act to protect the confidentiality and security of nonpublic personal information about consumers. Savings associations that do not disclose nonpublic personal information about consumers to nonaffiliated third parties may provide relatively simple initial and annual notices to their customers.

OTS recognizes that the Congressional Conferees on the Act wished to ensure that smaller financial institutions are not placed at a competitive disadvantage by a statutory regime that permits certain information to be shared freely within an affiliate structure while limiting the ability to share that same information with nonaffiliated third parties. The Conferees stated that, in prescribing regulations, the federal regulatory agencies should take into consideration any adverse competitive effects upon small commercial banks, thrifts, and credit unions. [16] At this time, it is not clear the extent to which small institutions will be placed at a disadvantage by information-sharing among affiliates in large institutional families. OTS believes that further experience under the regulation would be appropriate before considering any exemptions in this area for small institutions.

To reduce regulatory burden, consistent with the statutory requirements, this proposed regulation would provide financial institutions with substantial flexibility to use privacy practices tailored to their individual needs. For example, the Agencies considered setting a certain time within which financial institutions that receive opt out notices must comply with them. Because the Agencies thought a certain time limit might impose undue regulatory burden, the proposed rule would require compliance with opt out notices ''as soon as reasonably practicable.'' § 573.8(e). Similarly, the proposed rule would become effective on November 13, 2000. This is designed to allow financial institutions one year after G–L–B was enacted, and six months after this rule's expected effective date, to come into compliance. § 573.16(a). The Agencies are soliciting comments on whether these time limits would allow financial institutions sufficient time to comply with the rules.

OTS requests comment on the burdens associated with the proposed rule and whether any exceptions for small institutions would be appropriate.

E. Other Matters

While the scope of the proposed regulation (pursuant to the G–L–B Act) is unique, there may be some overlap in certain circumstances with certain Federal rules. As noted above, the Fair Credit Reporting Act requires a savings

[15] G–L–B Act, Pub. Law. No. 106–102, 113 Stat. 1338, § 501(a) (1999) (to be codified at 15 USC 6801).

[16] H. R. Conf. Rep. No. 106–434, at 173 (1999).

association that (1) does not want to be treated as a consumer reporting agency and (2) desires to share certain consumer information (*i.e.,* application or credit report information) with its affiliates, to provide the consumer with a clear and conspicuous notice and an opportunity to opt out of such information sharing. Also, at the time a consumer contracts for an electronic fund transfer service, the Electronic Funds Transfer Act requires the terms and conditions of such transfer to be disclosed, including under what circumstances the bank will in the ordinary course of business disclose information concerning the consumer's account to third persons. Finally, the Children's Online Privacy Protection Act (under which the Federal banking agencies are charged with enforcement of implementing regulations promulgated by the Federal Trade Commission) generally requires online service operators collecting personal information from a child to obtain parental consent and post a privacy notice on the web site. OTS seeks comment on additional Federal rules that may duplicate, overlap or conflict with the proposal.

C. Executive Order 12866

OCC: The Comptroller of the Currency has determined that this proposed rule, if adopted as a final rule, does not constitute a ''significant regulatory action'' for the purposes of Executive Order 12866. The rule follows closely the requirements of title V, subtitle A of the G–L–B Act. Since, the G–L–B Act establishes the minimum requirements for this activity, the OCC has little discretion to propose regulatory options that might significantly reduce costs or other burdens. However, even absent the requirements of the G–L–B Act, if the OCC issued the rule under its own authority, the rule would not constitute a ''significant regulatory action'' for the purposes of Executive Order 12866.

Nevertheless, the OCC acknowledges that the rule would impose costs on national banks by requiring them to make notifications and take other actions impacting their day to day operations. Therefore, the OCC invites national banks and the public to provide any cost estimates and related data that they think would be useful to the agency in evaluating the overall costs of the rule. The OCC will review carefully the comments and cost data that you provide and will revisit the cost aspects of the G–L–B Act as implemented by this proposal in developing the final rule.

OTS: OTS has determined that this proposed rule, if adopted as a final rule, would not constitute a ''significant regulatory action'' for the purposes of Executive Order 12866. The rule follows closely the requirements of title V, subtitle A of the G–L–B Act. Since the G–L–B Act establishes the minimum requirements for this activity, OTS has little discretion to propose regulatory options that might significantly reduce costs or other burdens.

Nevertheless, OTS acknowledges that the rule would impose costs on the thrift industry by requiring savings associations to make notifications and take other actions impacting their day to day operations. Therefore, OTS invites the thrift industry and the public to provide any cost estimates and related data that they think would be useful to the agency in evaluating the overall costs of the rule. OTS will review carefully the comments and cost data that you provide and will revisit the cost aspects of the G–L–B Act as implemented by this proposal in developing the final rule.

D. Unfunded Mandates Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1532 (Unfunded Mandates Act), requires that an agency prepare a budgetary impact statement before promulgating any rule likely to result in a Federal mandate that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. If a budgetary impact statement is required, section 205 of the Unfunded Mandates Act also requires the agency to identify and consider a reasonable number of regulatory alternatives before promulgating the rule. However, an agency is not required to assess the effects of its regulatory actions on the private sector to the extent that such regulations incorporate requirements specifically set forth in law. 2 U.S.C. 1531. Most of the proposed rule's provisions are already mandated by the applicable provisions in Title V of the G–L–B Act, which would become effective and binding on the private sector without a regulatory promulgation. Therefore, the OCC and OTS have determined that this proposed regulation will not result in expenditures by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. Accordingly, the OCC and OTS have not prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

V. Solicitation of Comments on Use of ''Plain Language''

Section 722 of the G–L–B Act requires the Federal banking agencies to use ''plain language'' in all proposed and final rules published after January 1, 2000. We invite your comments on how to make this proposed rule easier to understand. For example:

- Have we organized the material to suit your needs? If not, how could the material be better organized?
- Are the requirements in the rule clearly stated? If not, how could the rule be more clearly stated?
- Does the rule contain technical language or jargon that isn't clear? If not, which language requires clarification? For example, is the phrase ''opt out'' confusing to the average reader? Should the Agencies require financial institutions to use a different phrase in their notices, such as ''choose not to have information shared''?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the rule easier to understand? If so, what changes to the format would make the rule easier to understand?
- Would more (but shorter) sections be better? If so, which sections should be changed?
- What else could we do to make the rule easier to understand?
- The Agencies solicit comment on whether the inclusion of examples in the regulation is appropriate. Elevating the fact patterns to safe harbors in the rule may generate certain problems over time. For example, changes in technology or practices may ultimately impact the fact patterns contained in the examples and require changes to the regulation. Are there alternative methods to offer illustrative guidance of the concepts portrayed by the examples?

List of Subjects

12 CFR Part 40

Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 216

Banks, banking, Consumer protection, Federal Reserve System, Foreign banking, Holding companies, Information, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 332

Banks, banking, Privacy.

12 CFR Part 573

Consumer protection, Privacy, Savings associations.

Office of the Comptroller of the Currency

12 CFR Chapter I

Authority and Issuance

For the reasons set out in the joint preamble, the OCC proposes to amend chapter I of title 12 of the Code of Federal Regulations by adding a new part 40 to read as follows:

PART 40—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

40.1 Purpose and scope.
40.2 Rule of construction.
40.3 Definitions.
40.4 Initial notice to consumers of privacy policies and practices required.
40.5 Annual notice to customers required.
40.6 Information to be included in initial and annual notices of privacy policies and practices.
40.7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.
40.8 Form and method of providing opt out notice to consumers.
40.9 Exception to opt out requirements for service providers and joint marketing.
40.10 Exceptions to notice and opt out requirements for processing and servicing transactions.
40.11 Other exceptions to notice and opt out requirements.
40.12 Limits on redisclosure and reuse of information.
40.13 Limits on sharing of account number information for marketing purposes.
40.14 Protection of Fair Credit Reporting Act.
40.15 Relation to State laws.
40.16 Effective date; transition rule.

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

§ 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 consumers about its privacy policies and practices;

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

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to certain nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 40.9, 40.10, and 40.11.

(b) *Scope.* The rules established by this part apply only to nonpublic personal information about individuals who obtain financial products or services for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business purposes. This part applies to 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, District of Columbia 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.

§ 40.2 Rule of construction.

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

§ 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 contained in the notice.

(2) *Examples.* (i) The bank makes it notice reasonably understandable if, to the extent applicable, the bank:

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

(B) Uses short explanatory sentences and 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; and

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

(ii) The bank designs its notice to call attention to the nature and significance of the information contained in the notice if, to the extent applicable, 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; and

(C) Provides wide margins and ample line spacing.

(iii) If the bank provides a notice on the same form as another notice or other document, the bank designs its notice to call attention to the nature and significance of the information contained in the notice if the bank uses:

(A) Larger type size(s), boldface or italics in the text;

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

(C) Shading or sidebars to highlight the notice, whenever possible.

(c) *Collect* means to obtain information that is organized or retrievable on a personally identifiable basis, 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 the bank that is to be used primarily for personal, family or household purposes, and 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 by the bank or another financial institution.

(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 an ongoing advisory relationship.

(iv) An individual who negotiates a workout with a bank for a loan that the bank owns is a consumer regardless of whether the bank originally extended the loan to the individual.

(v) An individual who has a loan from a bank is the bank's consumer even if the bank:

(A) Hires an agent to collect on the loan;

(B) Sells the rights to service the loan; or

(C) Bought the loan from the financial institution that originated the loan.

(vi) An individual is not a bank's consumer solely because the bank processes information about the individual on behalf of a financial institution that extended the loan to the individual.

(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 determined by the OCC.

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

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

(B) Purchases an insurance product from the bank;

(C) Holds an investment product through the bank;

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

(E) Has a loan that the bank services where the bank owns the servicing rights;

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

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

(ii) A consumer does not, however, have a continuing relationship with a bank if:

(A) The consumer only obtains a financial product or service in an isolated transaction, such as withdrawing cash from the bank's automated teller machine (ATM) 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 an isolated transaction.

(j) (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.

(k) (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, brokerage or distribution of information that the bank collects in connection with a request or an application from a consumer for a financial product or service.

(l) *Government regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission;

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

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

(9) The Federal Trade Commission.

(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 by virtue of the direct or indirect ownership or control of the company by the financial institution or any affiliate of the financial institution in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

Alternative A

(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.

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

(3) *Example.* Nonpublic personal information includes any list of individuals' street addresses and telephone numbers that is derived using any information consumers provide to you on an application for a financial product or service.

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

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

(ii) 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, other than publicly available information.

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

(A) Information a consumer provides to a bank on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

(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 a bank's customers or has obtained a financial product or service from the bank, unless that fact is derived using only publicly available information, such as government real estate records or bankruptcy records;

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

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

(F) Information from a consumer report.

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

(p) (1) *Publicly available information* means any information that is lawfully made available to the general public that is obtained from:

(i) Federal, State or local government records;

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

Alternative B

(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.

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

(i) Publicly available information, except as provided in paragraph (n)(1)(ii) of this section; or

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

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

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

(i) Provided by a consumer 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 the 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) Personally identifiable financial information includes:

(A) Information a consumer provides to a bank on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

(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, unless that fact is derived using only publicly available information, such as government real estate records or bankruptcy records;

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

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

(F) Information from a consumer report.

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

(p) (1) *Publicly available information* means any information that is lawfully made available to the general public from:

(i) Federal, State or local government records;

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

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

(a) *When initial notice is required.* A bank must provide a clear and conspicuous notice that accurately reflects the bank's privacy policies and practices to:

(1) An individual who becomes the bank's customer, prior to the time that the bank establishes a customer relationship, except as provided in paragraph (d)(2) of this section; and

(2) A consumer, prior to the time that a 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 §§ 40.10 and 40.11.

(b) *When initial notice to a consumer is not required.* The bank is not required to provide an initial notice to a consumer under paragraph (a)(1) 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 §§ 40.10 and 40.11; 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 at the time the bank and the consumer enter into a continuing relationship.

(2) *Examples.* The bank establishes a customer relationship when the consumer:

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

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

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

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

(d) *How to provide notice*—(1) *General rule.* A bank must provide the privacy notice required by paragraph (a) of this section so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form.

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

(i) The bank purchases a loan or assumes a deposit liability from another financial institution and the customer of that loan or deposit account does not have a choice about the bank's purchase or assumption; or

(ii) The bank and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice thereafter.

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

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

(5) *Examples.* (i) A bank may reasonably expect that a consumer will receive actual notice of its privacy policies and practices if the bank:

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

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

(C) 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;

(D) 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.

(ii) A bank may *not,* however, reasonably expect that a consumer will receive actual notice of the bank's privacy policies and practices if the bank:

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

(B) Sends the notice via electronic mail to a consumer who obtains a financial product or service from the bank in person or through the mail and who does not agree to receive the notice electronically.

(iii) A bank provides the initial privacy notice to the customer so that it can be retained or obtained at a later time if the bank:

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

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

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

§ 40.5 Annual notice to customers required.

(a) *General rule.* A bank must provide a clear and conspicuous notice to customers that accurately reflects the bank's 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.

(b) *How to provide notice.* A bank must provide the annual notice required by paragraph (a) of this section to a customer using a means permitted for providing the initial notice to that customer under § 40.4(d).

(c) (1) *Termination of customer relationship.* A bank is not required to provide an annual notice to a customer with whom the bank no longer has a continuing relationship.

(2) *Examples.* A bank no longer has a continuing relationship with an individual if:

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

(ii) In the case of a closed-end loan, the consumer 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 consumer concerning that relationship or the bank sells the credit card receivables without retaining servicing rights; or

(iv) For other types of relationships, the bank has not communicated with the consumer about the relationship for a period of 12 consecutive months, other than to provide annual notices of privacy policies and practices.

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

(a) *General rule.* The initial and annual notices that a bank provides about its privacy policies and practices under §§ 40.4 and 40.5 must include each of the following items of information:

(1) The categories of nonpublic personal information about the bank's consumers that the bank collects;

(2) The categories of nonpublic personal information about the bank's consumers that the bank discloses;

(3) The categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information about its consumers, other than those parties to whom the bank discloses information under §§ 40.10 and 40.11;

(4) The categories of nonpublic personal information about the bank's former customers that it discloses and the categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information about its former customers, other than those parties to whom it discloses information under §§ 40.10 and 40.11;

(5) If the bank discloses nonpublic personal information to a nonaffiliated third party under § 40.9 (and no other exception applies to that disclosure), a separate description 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 right under § 40.8(a) of the consumer to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;

(7) Any disclosures that 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); and

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

(b) *Description of nonaffiliated third parties subject to exceptions.* If a bank discloses nonpublic personal information about a consumer to third parties as authorized under §§ 40.10 and 40.11, the bank is 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, the bank is only required to state that it makes disclosures to other nonaffiliated third parties as permitted by law.

(c) *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 does 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.

(d) *Examples*—(1) *Categories of nonpublic personal information that the bank collects.* A bank adequately categorizes the nonpublic personal information it collects if it categorizes the information according to the source of the information, such as application information, information about transactions (such as information regarding a deposit, loan, or credit card account), and consumer reports.

(2) *Categories of nonpublic personal information the bank discloses.* A bank adequately categorizes nonpublic personal information it discloses if the bank categorizes the information according to source, and provides illustrative examples of the content of the information. These might include application information, such as assets and income; identifying information, such as name, address, and social security number; and transaction information, such as information about account balance, payment history, parties to the transaction, and credit card usage; and information from consumer reports, such as a consumer's creditworthiness and credit history. A bank does not adequately categorize the information that it discloses if it uses only general terms, such as transaction information about the consumer.

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

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

(5) *Confidentiality, security, and integrity.* A bank adequately describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if it explains who has access to the information and the circumstances under which the information may be accessed. The bank adequately describes its policies and practices with respect to protecting the integrity of nonpublic personal information if it explains measures the bank takes to protect against reasonably anticipated threats or hazards. A bank is not required to describe technical information about the safeguards the bank uses.

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

(a) (1) *Conditions for disclosure.* Except as otherwise authorized in this part, 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 § 40.8;

(iii) The bank has given the consumer a reasonable opportunity, before the time that the bank 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 §§ 40.9, 40.10, and 40.11.

(3) *Examples of reasonable opportunity to opt out*—(i) *By mail.* A bank provides a consumer with whom it has a customer relationship with a reasonable opportunity to opt out if the bank mails the notices required in paragraph (a)(1) of this section to the consumer and allows the consumer a reasonable period of time, such as 30 days, to opt out.

(ii) *Isolated transaction with a consumer.* For an isolated transaction, such as the purchase of a cashier's check by a consumer, a bank provides a reasonable opportunity to opt out if the bank provides the consumer with the required notices 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, it may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that the bank has collected, regardless of whether it collected the information 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.

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

(a)(1) *Form of opt out notice.* A bank must provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under § 40.7(a)(1). 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) 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 identifies all of the categories of nonpublic personal information that the bank discloses or reserves the right to disclose to nonaffiliated third parties as described in § 40.6 and states that the consumer can opt out of the disclosure of that information.

(ii) A bank provides a reasonable means of opting out 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; or

(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.

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

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

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

(3) *Same form as initial notice permitted.* 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.

(4) *Initial notice required when opt out notice delivered subsequent to initial notice.* If the bank provides the opt out notice at a later time than required for the initial notice in accordance with § 40.4, the bank must also include a copy of the initial notice in writing or, if the consumer agrees, in an electronic form with the opt out notice.

(c) *Notice of change in terms*—(1) *General rule.* Except as otherwise authorized in this part, the 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 the consumer under § 40.4, unless:

(i) The bank has provided to the consumer a revised notice that accurately describes the bank's policies and practices;

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

(iii) The bank has given the consumer a reasonable opportunity, before the time that the bank discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) *How to provide notice of change in terms.* A bank must provide the revised notice of its policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under § 40.4(d) and paragraph (b) of this section, respectively.

(3) *Examples*—(i) Except as otherwise permitted by §§ 40.9,40.10 and 40.11, a change-in-terms notice is required if a bank:

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

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

(ii) A change-in-terms notice is not required if a bank discloses nonpublic personal information to a new nonaffiliated third party that is adequately described by the bank's prior notice.

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

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

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

(a) *General rule.* The opt out requirements in §§ 40.7 and 40.8 do not apply when a bank provides nonpublic personal information about a consumer to a nonaffiliated third party to perform services for the bank or functions on the bank's behalf, if the bank:

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

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

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

(ii) Limits the third party's use of information the bank discloses solely to the purposes for which the information is disclosed or as otherwise permitted by §§ 40.10 and 40.11 of this part.

(b) *Service may include joint marketing.* The services performed for a bank by a nonaffiliated third party 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.

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

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 40.4(a)(2), the opt out in §§ 40.7 and 40.8 and service providers and joint marketing in § 40.9 do not apply if the bank discloses nonpublic personal information:

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

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

(3) To maintain or service the consumer's account with the 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

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

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

(1) Required, or is one of the lawful or appropriate methods, to enforce 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 the 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 settling a transaction, including:

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

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

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

§ 40.11 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 40.8 and service providers and joint marketing in § 40.9 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 the 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 the 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 government regulators), self-regulatory organizations, or for an investigation on a matter related to public safety;

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

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

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

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

(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 the 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 § 40.8(d).

§ 40.12 Limits on redisclosure and reuse of information.

(a) *Limits on the bank's redisclosure and reuse.* (1) Except as otherwise provided in this part, if a bank receives nonpublic personal information about a consumer from a nonaffiliated financial institution, the bank must not, directly or through an affiliate, disclose the information to any other person that is not affiliated with either the bank or the other financial institution, unless the disclosure would be lawful if the financial institution made it directly to such other person.

(2) A bank may use nonpublic personal information about a consumer that it receives from a nonaffiliated financial institution in accordance with an exception under §§ 40.9, 40.10, or 40.11 only for the purpose of that exception.

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

(2) A nonaffiliated third party may use nonpublic personal information about a consumer that it receives from a bank in accordance with an exception under §§ 40.9, 40.10, or 40.11 only for the purpose of that exception.

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

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 credit card account, deposit account or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

§ 40.14 Protection of Fair Credit Reporting Act.

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

§ 40.15 Relation to State laws.

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

§ 40.16 Effective date; transition rule.

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

(b) *Notice requirement for consumers who were customers on the effective*

date. No later than 30 days after the effective date of this part, a bank must provide an initial notice, as required by § 40.4, to consumers who were the bank's customers on the effective date of this part.

Dated: February 2, 2000.

John D. Hawke, Jr.,

Comptroller of the Currency.

Board of Governors of the Federal Reserve System

12 CFR Chapter II

Authority and Issuance

For the reasons set out in the joint preamble, Title 12, Chapter II, of the Code of Federal Regulations is proposed to be amended by adding a new part 216 to read as follows:

PART 216—PRIVACY OF CONSUMER FINANCIAL INFORMATION (REGULATION P)

Sec.

216.1 Purpose and scope.
216.2 Rule of construction.
216.3 Definitions.
216.4 Initial notice to consumers of privacy policies and practices required.
216.5 Annual notice to customers required.
216.6 Information to be included in initial and annual notices of privacy policies and practices.
216.7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.
216.8 Form and method of providing opt out notice to consumers.
216.9 Exception to opt out requirements for service providers and joint marketing.
216.10 Exceptions to notice and opt out requirements for processing and servicing transactions.
216.11 Other exceptions to notice and opt out requirements.
216.12 Limits on redisclosure and reuse of information.
216.13 Limits on sharing of account number information for marketing purposes.
216.14 Protection of Fair Credit Reporting Act.
216.15 Relation to State laws.
216.16 Effective date; transition rule.

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

§ 216.1 Purpose and scope.

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

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

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

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 216.9, 216.10, and 216.11.

(b) *Scope.* The rules established by this part apply only to nonpublic personal information about individuals who obtain financial products or services for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business purposes. This part applies to entities for which the Board has primary supervisory authority. They are referred to in this part as ''you.'' These are: State member banks, bank holding companies and certain of their nonbank subsidiaries or affiliates, State uninsured branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and Agreement corporations.

§ 216.2 Rule of construction.

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

§ 216.3 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 contained in the notice.

(2) *Examples.* (i) You make your notice reasonably understandable if, to the extent applicable, you:

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

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

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

(D) Avoid multiple negatives;

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

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

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

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

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

(C) Provide wide margins and ample line spacing.

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

(A) Larger type size(s), boldface or italics in the text;

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

(C) Shading or sidebars to highlight the notice, whenever possible.

(c) *Collect* means to obtain information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information.

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

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

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

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

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

(iv) An individual who negotiates a workout with you for a loan that you own is a consumer regardless of whether you originally extended the loan to the individual.

(v) An individual who has a loan from you is your consumer even if you:

(A) Hire an agent to collect on the loan;

(B) Sell the rights to service the loan; or

(C) Bought the loan from the financial institution that originated the loan.

(vi) An individual is not your consumer solely because you process information about the individual on behalf of a financial institution that extended the loan to the individual.

(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 determined by the Board.

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

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

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

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

(B) Purchases an insurance product from you;

(C) Holds an investment product through you;

(D) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan for the consumer;

(E) Has a loan that you service where you own the servicing rights;

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

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

(ii) A consumer does not, however, have a continuing relationship with you if:

(A) The consumer only obtains a financial product or service in an isolated transaction, such as withdrawing cash from your ATM or purchasing a cashier's check or money order;

(B) You sell the consumer's loan and do not retain the rights to service that loan; or

(C) You sell the consumer airline tickets, travel insurance or traveler's checks in an isolated transaction.

(j) (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.

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

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

(l) *Government regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission;

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

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

(9) The Federal Trade Commission.

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

(i) Your affiliate; or

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

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

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

(i) Personally identifiable financial information; and

(ii) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information.

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

(i) Publicly available information, except as provided 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.

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

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

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

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

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

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

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

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

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

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

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

(F) Information from a consumer report.

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

(p) (1) *Publicly available information* means any information that is lawfully made available to the general public from:

(i) Federal, State or local government records;

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

(q) *You* means:

(1) A State member bank, as defined in 12 CFR 208.3(g) and its subsidiaries;

(2) A bank holding company, as defined in 12 CFR 225.2(c);

(3) A subsidiary (as defined in 12 CFR 225.2(o)) or affiliate of a bank holding company, except for a:

(i) National bank or a State bank that is not a member of the Federal Reserve System;

(ii) Broker, as defined in 15 U.S.C. 78c(a)(4);

(iii) Dealer, as defined in 15 U.S.C. 78c(a)(5);

(iv) Person, to the extent that person is engaged in the business of insurance in a State as principal or agent and required to be licensed by the appropriate State insurance authority;

(v) Investment company, as defined in 15 U.S.C. 80a–3; or

(vi) Investment adviser, as defined in 15 U.S.C. 80b–2(a)(11);

(4) A State agency or State branch of a foreign bank, as those terms are defined in 12 U.S.C. 3101(b)(11) and (12), the deposits of which agency or branch are not insured by the Federal Deposit Insurance Corporation;

(5) A commercial lending company, as defined in 12 CFR 211.21(f), that is owned or controlled by a foreign bank, as defined in 12 CFR 211.21(m); or

(6) A corporation organized under section 25A of the Federal Reserve Act (12 U.S.C. 611–631) or a corporation having an agreement or undertaking with the Board under section 25 of the Federal Reserve Act (12 U.S.C. 601–604a).

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

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

(1) An individual who becomes your customer, prior to the time that you establish a customer relationship, except as provided in paragraph (d)(2) of this section; and

(2) A consumer, prior to the time that you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 216.10 and 216.11.

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

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 216.10 and 216.11; and

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

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

(2) *Examples.* You establish a customer relationship when the consumer:

(i) Opens a credit card account with you;

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

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

(iv) Becomes your client for the purpose of your providing credit counseling or tax preparation services.

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

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

(i) You purchase a loan or assume a deposit liability from another financial institution and the customer of that loan or deposit account does not have a choice about your purchase or assumption; or

(ii) You and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice thereafter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 216.5 Annual notice to customers required.

(a) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists.

(b) *How to provide notice.* You must provide the annual notice required by paragraph (a) of this section to a customer using a means permitted for providing the initial notice to that customer under § 216.4(d).

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

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

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

(ii) In the case of a closed-end loan, the consumer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;

(iii) In the case of a credit card relationship or other open-end credit relationship, you no longer provide any statements or notices to the consumer concerning that relationship or you sell the credit card receivables without retaining servicing rights; or

(iv) For other types of relationships, you have not communicated with the consumer about the relationship for a period of 12 consecutive months, other than to provide annual notices of privacy policies and practices.

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

(a) *General rule.* The initial and annual notices that you provide about your privacy policies and practices under §§ 216.4 and 216.5 must include each of the following items of information:

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your consumers, other than those parties to whom you disclose information under §§ 216.10 and 216.11;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 216.10 and 216.11;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 216.9 (and no other exception applies to that disclosure), a separate description of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the right under § 216.8(a) of the consumer to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;

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

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

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information about a consumer to third parties as authorized under §§ 216.10 and 216.11, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 216.4 and 216.5. When describing the categories with respect to those parties, you are only required to state that you make disclosures to other nonaffiliated third parties as permitted by law.

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

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

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

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

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

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

(4) *Simplified notices.* If you do not disclose, and do not intend to disclose,

nonpublic personal information to affiliates or nonaffiliated third parties, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), and (b) of this section.

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

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

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

(i) You have provided to the consumer an initial notice as required under § 216.4;

(ii) You have provided to the consumer an opt out notice as required in § 216.8;

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

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 216.9, 216.10 and 216.11.

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

(ii) *Isolated transaction with consumer.* For an isolated transaction, such as the purchase of a cashier's check by a consumer, you provide a reasonable opportunity to opt out if you provide the consumer with the required notices at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

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

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

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

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

(a)(1) *Form of opt out notice.* You must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under § 216.7(a)(1). The notice must state:

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

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

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

(2) *Examples.* (i) You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose to nonaffiliated third parties as described in § 216.6 and state that the consumer can opt out of the disclosure of that information.

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

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

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

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

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

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

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

(3) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 216.4.

(4) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice at a later time than required for the initial notice in accordance with § 216.4, you must also include a copy of the initial notice in writing or, if the consumer agrees, in an electronic form with the opt out notice.

(c) *Notice of change in terms*—(1) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to the consumer under § 216.4, unless:

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

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

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

(iv) The consumer does not opt out.

(2) *How to provide notice of change in terms.* You must provide the revised notice of your policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under § 216.4(d) and paragraph (b) of this section, respectively.

(3) *Examples.* (i) Except as otherwise permitted by §§ 216.9, 216.10 and 216.11, a change-in-terms notice is required if you:

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

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

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

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

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

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

(a) *General rule.* The opt out requirements in §§ 216.7 and 216.8 do not apply when you provide nonpublic personal information about a consumer to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(1) Provide the initial notice in accordance with § 216.4; and

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

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

(ii) Limits the third party's use of information you disclose solely to the purposes for which the information is disclosed or as otherwise permitted by §§ 216.10 and 216.11 of this part.

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

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

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

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 216.4(a)(2), the opt out in §§ 216.7 and 216.8 and service providers and joint marketing in § 216.9 do not apply if you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 216.11 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice to consumers in § 216.4(a)(2), the opt out in §§ 216.7 and 216.8, and service providers and joint marketing in § 216.9 do not apply when you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

concerns solely consumers of such business or unit; or

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

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

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

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to you for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 216.8(d).

§ 216.12 Limits on redisclosure and reuse of information.

(a) *Limits on your redisclosure and reuse.* (1) Except as otherwise provided in this part, if you receive nonpublic personal information about a consumer from a nonaffiliated financial institution, you must not, directly or through an affiliate, disclose the information to any other person that is not affiliated with either the financial institution or you, unless the disclosure would be lawful if the financial institution made it directly to such other person.

(2) You may use nonpublic personal information about a consumer that you receive from a nonaffiliated financial institution in accordance with an exception under §§ 216.9, 216.10 or 216.11 only for the purpose of that exception.

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

(2) A nonaffiliated third party may use nonpublic personal information about a consumer that it receives from you in accordance with an exception under §§ 216.9, 216.10 or 216.11 only for the purpose of that exception.

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

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

§ 216.14 Protection of Fair Credit Reporting Act.

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

§ 216.15 Relation to State laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation in effect in any State, except to the extent that 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 Board, on the Federal Trade Commission's own motion or upon the petition of any interested party.

§ 216.16 Effective date; transition rule.

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

(b) *Notice requirement for consumers who were your customers on the effective date.* No later than thirty days after the effective date of this part, you must provide an initial notice, as required by § 216.4, to consumers who were your customers on the effective date of this part.

By order of the Board of Governors of the Federal Reserve System, February 10, 2000.

Jennifer J. Johnson,

Secretary of the Board.

Federal Deposit Insurance Corporation 12 CFR Chapter III

Authority and Issuance

For the reasons set out in the joint preamble, Title 12, Chapter III of the Code of Federal Regulations is proposed to be amended by adding a new part 332 to read as follows:

PART 332—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

332.1 Purpose and scope.
332.2 Rule of construction.
332.3 Definitions.
332.4 Initial notice to consumers of privacy policies and practices required.
332.5 Annual notice to customers required.
332.6 Information to be included in initial and annual notices of privacy policies and practices.
332.7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.
332.8 Form and method of providing opt out notice to consumers.
332.9 Exception to opt out requirements for service providers and joint marketing.
332.10 Exceptions to notice and opt out requirements for processing and servicing transactions.
332.11 Other exceptions to notice and opt out requirements.
332.12 Limits on redisclosure and reuse of information.
332.13 Limits on sharing of account number information for marketing purposes.
332.14 Protection of Fair Credit Reporting Act.
332.15 Relation to State laws.
332.16 Effective date; transition rule.

Authority: 12 U.S.C. 1819 (Seventh and Tenth); 15 U.S.C. 6801 *et seq.*

§ 332.1 Purpose and scope.

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

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

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

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to certain nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 332.9, 332.10, and 332.11.

(b) *Scope.* The rules established by this part apply only to nonpublic personal information about individuals who obtain financial products or services for personal, family or household purposes from the institutions listed in this paragraph (b). This part does not apply to information about companies or about individuals who obtain financial products or services for business purposes. This part applies to entities for which the Federal Deposit Insurance Corporation has primary supervisory authority. They are referred to in this part as ''you.'' These are banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured state branches 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.

§ 332.2 Rule of construction.

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

§ 332.3 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 contained in the notice.

(2) *Examples.* (i) You make your notice reasonably understandable if, to the extent applicable, you:

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

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

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

(D) Avoid multiple negatives;

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

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

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

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

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

(C) Provide wide margins and ample line spacing.

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

(A) Larger type size(s), boldface or italics in the text;

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

(C) Shading or sidebars to highlight the notice, whenever possible.

(c) *Collect* means to obtain information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information.

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

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

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

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

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

(iv) An individual who negotiates a workout with you for a loan that you own is a consumer regardless of whether you originally extended the loan to the individual.

(v) An individual who has a loan from you is your consumer even if you:

(A) Hire an agent to collect on the loan;

(B) Sell the rights to service the loan; or

(C) Bought the loan from the financial institution that originated the loan.

(vi) An individual is not your consumer solely because you process information about the individual on behalf of a financial institution that extended the loan to the individual.

(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 determined by the FDIC.

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

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

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

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

(B) Purchases an insurance product from you;

(C) Holds an investment product through you;

(D) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan for the consumer;

(E) Has a loan that you service where you own the servicing rights;

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

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

(ii) A consumer does not, however, have a continuing relationship with you if:

(A) The consumer only obtains a financial product or service in an

isolated transaction, such as withdrawing cash from your ATM or purchasing a cashier's check or money order;

(B) You sell the consumer's loan and do not retain the rights to service that loan; or

(C) You sell the consumer airline tickets, travel insurance or traveler's checks in an isolated transaction.

(j) (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.

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

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

(l) *Government regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission;

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

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

(9) The Federal Trade Commission.

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

(i) Your affiliate; or

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

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

Alternative A

(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.

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

(3) *Example.* Nonpublic personal information includes any list of individuals' street addresses and telephone numbers that is derived using any information consumers provide to you on an application for a financial product or service.

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

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

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

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer, other than publicly available information.

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

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

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

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

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

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

(F) Information from a consumer report.

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

(p) (1) *Publicly available information* means any information that is lawfully made available to the general public that is obtained from:

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

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

Alternative B

(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.

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

(i) Publicly available information, except as provided 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.

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

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

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

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

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

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

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

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

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

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

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

(F) Information from a consumer report.

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

(p)(1) *Publicly available information* means any information that is lawfully made available to the general public from:

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

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

(q) *You* means a bank insured by the Federal Deposit Insurance Corporation (other than a member of the Federal Reserve System), an insured state branch of a foreign bank, and any subsidiary of either such entity except:

(1) A broker, as defined in 15 U.S.C. 78c(a)(4);

(2) A dealer, as defined in 15 U.S.C. 78c(a)(5);

(3) A person, to the extent that person is engaged in the business of insurance in a State as principal or agent and required to be licensed by the appropriate State insurance authority;

(4) An investment company, as defined in 15 U.S.C. 80a–3(a)(1); or

(5) An investment adviser, as defined in 15 U.S.C. 80b–2(a)(20).

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

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

(1) An individual who becomes your customer, prior to the time that you establish a customer relationship, except as provided in paragraph (d)(2) of this section; and

(2) A consumer, prior to the time that you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 332.10 and 332.11.

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

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 332.10 and 332.11; and

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

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

(2) *Examples.* You establish a customer relationship when the consumer:

(i) Opens a credit card account with you;

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

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

(iv) Becomes your client for the purpose of your providing credit counseling or tax preparation services.

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

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

(i) You purchase a loan or assume a deposit liability from another financial institution and the customer of that loan or deposit account does not have a choice about your purchase or assumption; or

(ii) You and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice thereafter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 332.5 Annual notice to customers required.

(a) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists.

(b) *How to provide notice.* You must provide the annual notice required by paragraph (a) of this section to a customer using a means permitted for providing the initial notice to that customer under § 332.4(d).

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

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

(i) In the case of a deposit account, the account is dormant under your policies;

(ii) In the case of a closed-end loan, the consumer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;

(iii) In the case of a credit card relationship or other open-end credit relationship, you no longer provide any statements or notices to the consumer concerning that relationship or you sell the credit card receivables without retaining servicing rights; or

(iv) For other types of relationships, you have not communicated with the consumer about the relationship for a period of 12 consecutive months, other than to provide annual notices of privacy policies and practices.

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

(a) *General rule.* The initial and annual notices that you provide about your privacy policies and practices under §§ 332.4 and 332.5 must include each of the following items of information:

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your consumers, other than those parties to whom you disclose information under §§ 332.10 and 332.11;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 332.10 and 332.11;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 332.9 (and no other exception applies to that disclosure), a separate description of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the right under § 332.8(a) of the consumer to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;

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

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

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information about a consumer to third parties as authorized under §§ 332.10 and 332.11, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 332.4 and 332.5. When describing the categories with respect to those parties, you are only required to state that you make disclosures to other nonaffiliated third parties as permitted by law.

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

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

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

(d) *Examples*—(1) *Categories of nonpublic personal information that you collect.* You adequately categorize the nonpublic personal information you collect if you categorize the information according to the source of the information, such as application information, information about transactions (such as information regarding a deposit, loan, or credit card account), and consumer reports.

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

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.* You adequately categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic

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

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

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

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

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

(i) You have provided to the consumer an initial notice as required under § 332.4;

(ii) You have provided to the consumer an opt out notice as required in § 332.8;

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

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 332.9, 332.10, and 332.11.

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

(ii) *Isolated transaction with a consumer.* For an isolated transaction, such as the purchase of a cashier's check by a consumer, you provide a reasonable opportunity to opt out if you provide the consumer with the required notices at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

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

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

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

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

(a) (1) *Form of opt out notice.* You must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under § 332.7(a)(1). The notice must state:

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

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

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

(2) *Examples.* (i) You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose to nonaffiliated third parties as described in § 332.6 and state that the consumer can opt out of the disclosure of that information.

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

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

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

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

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

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

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

(3) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 332.4.

(4) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice at a later time than required for the initial notice in accordance with § 332.4, you must also include a copy of the initial notice in writing or, if the consumer agrees, in an electronic form with the opt out notice.

(c) *Notice of change in terms*—(1) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to the consumer under § 332.4, unless:

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

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

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

(iv) The consumer does not opt out.

(2) *How to provide notice of change in terms.* You must provide the revised notice of your policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under § 332.4(d) and paragraph (b) of this section, respectively.

(3) *Examples.* (i) Except as otherwise permitted by §§ 332.9, 332.10, and 332.11, a change-in-terms notice is required if you:

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

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

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

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

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

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

(a) *General rule.* The opt out requirements in §§ 332.7 and 332.8 do not apply when you provide nonpublic personal information about a consumer to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(1) Provide the initial notice in accordance with § 332.4; and

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

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

(ii) Limits the third party's use of information you disclose solely to the purposes for which the information is disclosed or as otherwise permitted by §§ 332.10 and 332.11 of this part.

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

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

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

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 332.4(a)(2), the opt out in §§ 332.7 and 332.8 and service providers and joint marketing in § 332.9 do not apply if you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 332.11 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice to consumers in § 332.4(a)(2), the opt out in §§ 332.7 and 332.8 and service providers and joint marketing in § 332.9 do not apply when you disclose nonpublic personal information:

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

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

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

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

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

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

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

(4) To the extent specifically permitted or required under other

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

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

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

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

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

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

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

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to you for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 332.8(d).

§ 332.12 Limits on redisclosure and reuse of information.

(a) *Limits on your redisclosure and reuse.* (1) Except as otherwise provided in this part, if you receive nonpublic personal information about a consumer from a nonaffiliated financial institution, you must not, directly or through an affiliate, disclose the information to any other person that is not affiliated with either you or the other financial institution, unless the disclosure would be lawful if the financial institution made it directly to such other person.

(2) You may use nonpublic personal information about a consumer that you receive from a nonaffiliated financial institution in accordance with an exception under §§ 332.9, 332.10, or 332.11 only for the purpose of that exception.

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

(2) A nonaffiliated third party may use nonpublic personal information about a consumer that it receives from you in accordance with an exception under §§ 332.9, 332.10, or 332.11 only for the purpose of that exception.

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

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

§ 32.14 Protection of Fair Credit Reporting Act.

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

§ 332.15 Relation to State laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation in effect in any State, except to the extent that 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 FDIC, on the Federal Trade Commission's own motion or upon the petition of any interested party.

§ 332.16 Effective date; transition rule.

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

(b) *Notice requirement for consumers who were customers on the effective date.* No later than 30 days after the effective date of this part, you must provide an initial notice, as required by § 332.4, to consumers who were your customers on the effective date of this part.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Dated at Washington, DC, this 9th day of February, 2000.

Robert E. Feldman,

Executive Secretary.

OFFICE OF THRIFT SUPERVISION

12 CFR Chapter V

Authority and Issuance

For the reasons set out in the joint preamble, OTS proposes to amend Chapter V of Title 12 of the Code of Federal regulations by adding part 573 to read as follows:

PART 573—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

573.1 Purpose and scope.
573.2 Rule of construction.
573.3 Definitions.
573.4 Initial notice to consumers of privacy policies and practices required.
573.5 Annual notice to customers required.
573.6 Information to be included in initial and annual notices of privacy policies and practices.
573.7 Limitation on disclosure of nonpublic personal information about consumers to nonaffiliated third parties.
573.8 Form and method of providing opt out notice to consumers.
573.9 Exception to opt out requirements for service providers and joint marketing.
573.10 Exceptions to notice and opt out requirements for processing and servicing transactions.
573.11 Other exceptions to notice and opt out requirements.
573.12 Limits on redisclosure and reuse of information.
573.13 Limits on sharing of account number information for marketing purposes.
573.14 Protection of Fair Credit Reporting Act.
573.15 Relation to State laws.
573.16 Effective date; transition rule.

Authority: 12 U.S.C. 1462a, 1463, 1464, 1828; 15 U.S.C. 6801 *et seq.*

§ 573.1 Purpose and scope.

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

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

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

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 573.9, 573.10, and 573.11.

(b) *Scope.* The rules established by this part apply only to nonpublic personal information about individuals who obtain financial products or services for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business purposes. This part applies to savings associations whose deposits are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations, but not to subsidiaries that are brokers, dealers, persons providing insurance, investment companies, or investment advisers. This part refers to these entities as ''you.''

§ 573.2 Rule of construction.

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

§ 573.3 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 contained in the notice.

(2) *Examples.* (i) You make your notice reasonably understandable if, to the extent applicable, you:

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

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

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

(D) Avoid multiple negatives;

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

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

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

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

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

(C) Provide wide margins and ample line spacing.

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

(A) Larger type size(s), boldface or italics in the text;

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

(C) Shading or sidebars to highlight the notice, whenever possible.

(c) *Collect* means to obtain information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information.

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

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

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

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

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

(iv) An individual who negotiates a workout with you for a loan that you own is a consumer regardless of whether you originally extended the loan to the individual.

(v) An individual who has a loan from you is your consumer even if you:

(A) Hire an agent to collect on the loan;

(B) Sell the rights to service the loan; or

(C) Bought the loan from the financial institution that originated the loan.

(vi) An individual is not your consumer solely because you process information about the individual on behalf of a financial institution that extended the loan to the individual.

(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 determined by OTS.

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

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

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

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

(B) Purchases an insurance product from you;

(C) Holds an investment product through you;

(D) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan for the consumer;

(E) Has a loan that you service where you own the servicing rights;

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

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

(ii) A consumer does not, however, have a continuing relationship with you if:

(A) The consumer only obtains a financial product or service in an isolated transaction, such as withdrawing cash from your ATM or purchasing a cashier's check or money order;

(B) You sell the consumer's loan and do not retain the rights to service that loan; or

(C) You sell the consumer travel insurance or traveler's checks in an isolated transaction.

(j) (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.

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

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

(l) *Government regulator* means:

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

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

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

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

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission;

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

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

(9) The Federal Trade Commission.

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

(i) Your affiliate; or

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

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

Alternative A

(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.

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

(3) *Example.* Nonpublic personal information includes any list of individuals' street addresses and telephone numbers that is derived using any information consumers provide to you on an application for a financial product or service.

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

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

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

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer, other than publicly available information.

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

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

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

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

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

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

(F) Information from a consumer report.

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

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

(i) Federal, State or local government records;

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

Alternative B

(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.

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

(i) Publicly available information, except as provided 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.

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

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

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

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

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

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

(A) Information a consumer provides to you on an application to obtain a loan, credit card, insurance or other financial product or service, including, among other things, medical information;

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

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

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

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

(F) Information from a consumer report.

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

(p)(1) *Publicly available information* means any information that is lawfully made available to the general public from:

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

(ii) Widely distributed media; or

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

(2) *Examples*—(i) *Government records.* Publicly available information contained in government records includes information contained in government real estate records 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 an Internet site that is available to the general public without requiring a password or similar restriction.

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

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

(1) An individual who becomes your customer, prior to the time that you establish a customer relationship, except as provided in paragraph (d)(2) of this section; and

(2) A consumer, prior to the time that you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 573.10 and 573.11.

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

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 573.10 and 573.11; and

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

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

(2) *Examples.* You establish a customer relationship when the consumer:

(i) Opens a credit card account with you;

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

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

(iv) Becomes your client for the purpose of your providing credit counseling or tax preparation services.

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

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

(i) You purchase a loan or assume a deposit liability from another financial institution and the customer of that loan or deposit account does not have a choice about your purchase or assumption; or

(ii) You and the consumer orally agree to enter into a customer relationship and the consumer agrees to receive the notice thereafter.

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

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

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

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

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

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

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

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

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

(B) Send the notice via electronic mail to a consumer who obtains a financial

product or service with you in person or through the mail and who does not agree to receive the notice electronically.

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

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

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

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

§ 573.5 Annual notice to customers required.

(a) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists.

(b) *How to provide notice.* You must provide the annual notice required by paragraph (a) of this section to a customer using a means permitted for providing the initial notice to that customer under § 573.4(d).

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

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

(i) In the case of a deposit account, the account is dormant under your policies;

(ii) In the case of a closed-end loan, the consumer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;

(iii) In the case of a credit card relationship or other open-end credit relationship, you no longer provide any statements or notices to the consumer concerning that relationship or you sell the credit card receivables without retaining servicing rights; or

(iv) For other types of relationships, you have not communicated with the consumer about the relationship for a period of 12 consecutive months, other than to provide annual notices of privacy policies and practices.

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

(a) *General rule.* The initial and annual notices that you provide about your privacy policies and practices under §§ 573.4 and 573.5 must include each of the following items of information:

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your consumers, other than those parties to whom you disclose information under §§ 573.10 and 573.11;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 573.10 and 573.11;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 573.9 (and no other exception applies to that disclosure), a separate description of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the right under § 573.8(a) of the consumer to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right;

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

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

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information about a consumer to third parties as authorized under §§ 573.10 and 573.11, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 573.4 and 573.5. When describing the categories with respect to those parties, you are only required to state that you make disclosures to other nonaffiliated third parties as permitted by law.

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

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

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

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

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

(4) *Simplified notices.* If you do not disclose, and do not intend to disclose, nonpublic personal information to affiliates or nonaffiliated third parties, you may simply state that fact, in

addition to the information you must provide under paragraphs (a)(1), (a)(8), and (b) of this section.

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

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

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

(i) You have provided to the consumer an initial notice as required under § 573.4;

(ii) You have provided to the consumer an opt out notice as required in § 573.8;

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

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 573.9, 573.10 and 573.11.

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

(ii) *Isolated transaction with consumer.* For an isolated transaction, such as the purchase of a cashier's check by a consumer, you provide a reasonable opportunity to opt out if you provide the consumer with the required notices at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

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

(1) You must comply with this section, regardless of whether you and the consumer have established a customer relationship.

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

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

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

(a) (1) *Form of opt out notice.* You must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under § 573.7(a)(1). The notice must state:

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

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

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

(2) *Examples.* (i) You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose to nonaffiliated third parties as described in § 573.6 and state that the consumer can opt out of the disclosure of that information.

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

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

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

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

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

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

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

(3) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 573.4.

(4) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice at a later time than required for the initial notice in accordance with § 573.4, you must also include a copy of the initial notice in writing or, if the consumer agrees, in an electronic form with the opt out notice.

(c) *Notice of change in terms—*(1) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to the consumer under § 573.4, unless:

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

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

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

(iv) The consumer does not opt out.

(2) *How to provide notice of change in terms.* You must provide the revised notice of your policies and practices and opt out notice to a consumer using the means permitted for providing the initial notice and opt out notice to that consumer under § 573.4(d) or paragraph (b) of this section respectively.

(3) *Examples.* (i) Except as otherwise permitted by §§ 573.9, 573.10 and 573.11, a change-in-terms notice is required if you:

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

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

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

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

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

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

(a) *General rule.* The opt out requirements in §§ 573.7 and 573.8 do not apply when you provide nonpublic personal information about a consumer to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(1) Provide the initial notice in accordance with § 573.4; and

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

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

(ii) Limits the third party's use of information you disclose solely to the purposes for which the information is disclosed or as otherwise permitted by §§ 573.10 and 573.11 of this part.

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

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

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

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 573.4(a)(2), the opt out in §§ 573.7 and 573.8 and service providers and joint marketing in § 573.9 do not apply if you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 573.11 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice to consumers in § 573.4(a)(2), the opt out in §§ 573.7 and 573.8 and service providers and joint marketing in § 573.9 do not apply when you disclose nonpublic personal information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to you for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 573.8(d).

§ 573.12 Limits on redisclosure and reuse of information.

(a) *Limits on your redisclosure and reuse.* (1) Except as otherwise provided in this part, if you receive nonpublic personal information about a consumer from a nonaffiliated financial institution, you must not, directly or through an affiliate, disclose the information to any other person that is not affiliated with either the financial institution or you, unless the disclosure would be lawful if the financial institution made it directly to such other person.

(2) You may use nonpublic personal information about a consumer that you receive from a nonaffiliated financial institution in accordance with an exception under §§ 573.9, 573.10 or 573.11 only for the purpose of that exception.

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

(2) A nonaffiliated third party may use nonpublic personal information about a consumer that it receives from you in accordance with an exception under §§ 573.9, 573.10, or 573.11 only for the purpose of that exception.

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

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

§ 573.14 Protection of Fair Credit Reporting Act.

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

§ 573.15 Relation to State laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that 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 OTS, on the Federal Trade Commission's own motion or upon the petition of any interested party.

§ 573.16 Effective date; transition rule.

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

(b) *Notice requirement for consumers who were your customers on the effective date.* No later than 30 days after the effective date of this part, you must provide an initial notice, as required by § 573.4, to consumers who were your customers on the effective date of this part.

Dated: February 9, 2000.

By the Office of Thrift Supervision.

Ellen Seidman,

Director.

[FR Doc. 00–3718 Filed 2–18–00; 8:45 am]

BILLING CODES 4810–33–P; 6210–01–P; 6714–01–P; 6720–01–P