DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 40

[Docket No. 00-XX]

RIN 1557-AB77

BOARD OF GOVERNORS OF THE 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 (OCC), Treasury; Board of Governors of the

Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); and Office of Thrift Supervision (OTS), Treasury.

ACTION: Joint final rule.

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 publishing final privacy rules pursuant to section 504 of the Gramm-Leach-Bliley Act (the GLB 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 GLB 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 notice and opt-out requirements and the consumer has not elected to opt out of the disclosure. These final rules implement the requirements outlined above.

EFFECTIVE DATE: This joint rule is effective November 13, 2000. However, compliance will be optional until July 1, 2001.

FOR FURTHER INFORMATION CONTACT:

OCC: Amy Friend, Assistant Chief Counsel, (202) 874-5200; Jeffery Abrahamson, Attorney, Legislative and Regulatory Activities Division, (202) 874-5090, or 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, Office of the Comptroller of the Currency, 250 E Street, SW, Washington, D.C. 20219.

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, James H. Mann, Attorney, (202) 452-2412, or Minh-Duc T. Le, Attorney, (202) 452-3667, Division of Consumer and Community Affairs. For the hearing impaired only, contact , Janice Simms, Telecommunications Device for the Deaf (TDD) (202) 872-4984, Board of Governors of the Federal Reserve System, 20th and C Streets, NW, Washington, D.C. 20551.

FDIC: James K. Baebel, Senior Review Examiner, Division of Compliance and Consumer Affairs, (202) 736-0229; Deanna Caldwell, Community Affairs Officer, Division of Compliance and Consumer Affairs, (202) 736-0141; 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, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, D.C. 20429.

OTS: Christine Harrington, Counsel (Banking and Finance), (202) 906-7957, or 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. Overview of comments received

III. Section-by-section analysis

IV. Guidance for Certain Institutions

V. Regulatory Analysis

A. Paperwork Reduction Act

B. Regulatory Flexibility Act

C. Executive Order 12866

D. Unfunded Mandates Act of 1995

I. Background

On November 12, 1999, President Clinton signed the GLB Act (Pub. L. 106-102) into law. Subtitle A of Title V of the Act, captioned Disclosure of Nonpublic Personal Information (codified at 15 U.S.C. 6801 et seq.), 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 final rules to implement Subtitle A that are consistent and comparable to the extent possible, as is required by the statute.[1] The texts of the Agencies' proposed regulations are substantively identical, and differ only with respect to the citations of authority for each Agency's rulemaking and definitions appropriate for institutions within each Agency's primary jurisdiction.

II. Overview of comments received

On February 22, 2000, the Agencies published a joint notice of proposed rulemaking (the proposal or proposed rule) in the Federal Register (65 FR 8770).[2] The Agencies collectively received a total of 8,126 comments in response to the proposal, although many commenters sent copies of the same letter to each of the Agencies.[3] Of these, several thousand were received from individuals, virtually all of whom encouraged the Agencies to provide greater protection of individuals' financial privacy. Many individuals noted their concerns generally about the loss of privacy and the receipt of unwanted solicitations by marketers. A large number of individuals also requested the Agencies to

---

[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 final rules.

[2] The NCUA, FTC, and SEC published separate proposed rules on different dates. These proposed rules, which were consistent and comparable with the proposals published by the Agencies, appeared in the Federal Register at 65 FR 10988 (March 1, 2000) (NCUA), 65 FR 11174 (March 1, 2000) (FTC), and 65 FR 12354 (March 8, 2000) (SEC).

[3] The NCUA, FTC, and SEC received 99, 640, and 112 comments, respectively, in response to their proposed rules.

support legislation that the commenters believe would provide additional protections.

Several letters were received from members of Congress. In two letters signed by several members of the House of Representatives, the Agencies were encouraged to exercise their rulemaking authority to provide more protections than were proposed. Other Congressmen requested, in separate letters, that the Agencies (a) create an exception under limited circumstances to the prohibition against the sharing of account numbers for marketing purposes and (b) ensure that social security numbers are considered "nonpublic personal information."

Other comments were received from consumer groups and others advocating that the Agencies extend privacy protections in a number of ways, such as by requiring (a) financial institutions to provide consumers with access to their information maintained by the institutions and the opportunity to correct errors, (b) more detailed disclosures of the information collected and disclosed, and (c) disclosures of a financial institution's privacy policies and practices earlier in the process of establishing a customer relationship. In a letter signed by 33 State Attorneys General, the Agencies were requested to add certain consumer protections to the disclosure requirements and to the provision permitting financial institutions to enter into joint marketing agreements.

The majority of the remainder of comments received by the Agencies were from insured depository institutions or their representatives. These commenters offered a large number of suggested changes, with the most commonly advanced suggestions including: an extension of the effective date of the rule; an amendment to the definition of "nonpublic personal information" to focus more clearly on "financial" information; a streamlining of information required in the initial and annual disclosures; a clarification of how one or more of the statutory exceptions operate; an exclusion from, or clarification

of, the definitions of "consumer" and "customer" in various contexts; and the addition of flexibility to provide initial notices at some point other than "prior to" the time a customer relationship is established.

Representatives of a wide variety of other interests, including the health care industry, retail merchants, insurance companies, securities firms, private investigators, and higher education, also suggested changes to the proposed rule.

The Agencies have modified the proposed rule in light of the comments received. These comments, and the Agencies' responses thereto, are discussed in the following section-by-section analysis. As was done in the preamble discussion of the proposal, the citations are to sections only, leaving citations to the part numbers used by each Agency blank. Following the section-by-section analysis, the Agencies have provided guidance for certain institutions that is intended to provide additional guidance on how these institutions may comply with the rule in a way that avoids unnecessary burden.

III. Section-by-section analysis

As an initial matter, the Agencies note that the final rule, unlike the proposal, presents the various sections in subparts that consist of related sections. This change was made to group related concepts together and thereby make the rule easier to follow. A derivation table is included following this preamble to assist readers in locating provisions as set out in the proposal. The Agencies also have added an Appendix A to the final rule, setting out sample disclosures for financial institutions to consider.

§ __.1 Purpose and scope.

Proposed § __.1 identified the purposes and scope of the rules. As stated in the proposal, the

rule is intended to require a financial institution to provide notice to customers about its privacy policies and practices; to describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and to provide 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 various exceptions as stated in the rule. The Agencies invited 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.

Most of the comments received on this section focused on the scope of the rules. Several commenters suggested that the Agencies clarify how the rule applies to insurance companies. The Agencies note that section 505 of GLB Act, which sets out the enforcement authority of the Agencies, extends this authority to subsidiaries of entities within each Agency's primary jurisdiction. That section then explicitly excludes "persons providing insurance" from each Agency's enforcement authority (and, by operation of section 504(a)(1) of GLB Act, from the Agencies' rulemaking authority). The Agencies affected by this provision have concluded that the exclusion of "persons providing insurance" is not intended to remove insurance activities conducted directly by an insured depository institution from the scope of the rule. Consistent with this reading of the statute, each Agency's final rule states that the exclusion of persons providing insurance applies only to persons doing so in a subsidiary of an entity within the primary jurisdiction of that Agency. See § 40.1(b) (OCC rule); § 216.3(q) (Board rule); and § 332.3(q) (FDIC rule). The OTS notes that, while it regulates savings and loan holding companies, a different Federal functional regulator, a state insurance authority, or the FTC may enforce privacy rules as to that holding company, under § 505 of the Act, depending on the nature of a savings

and loan holding company's activities.

Several other commenters asked that the final rule state that certain transactions that are exempt from the coverage of the Truth in Lending Act (TILA; 15 U.S.C. 1601 et seq.) and Regulation Z (Reg. Z, 12 CFR part 226) also be treated as beyond the scope of the privacy rule. TILA and Reg. Z, which impose disclosure requirements on credit extended to consumers under certain circumstances, exempt several transactions, including those involving business, commercial, or agricultural credit. 15 U.S.C. 1603(1); 12 CFR 226.3(a). The Agencies agree that transactions that fit within the exemptions from TILA and Reg. Z for these types of credit also would fall outside the scope of the privacy rule, and have amended § __.1(b) accordingly. Thus, financial institutions may look at how this exemption is applied under Reg. Z for guidance on the scope of covered transactions under the privacy rule. It should be noted, however, that TILA exempts several other types of transactions that would be covered under the privacy rule if they are for the purpose of an individual obtaining a financial product or service as that term is defined in the privacy regulation. See 15 U.S.C. 1603(2) and (3).

A few commenters stated that the rule should apply to foreign entities who solicit business from people in the United States. The OCC, FRB, and FDIC each have been given explicit authority to enforce the privacy rule with respect to foreign institutions within their respective jurisdictions that have offices in the U.S. Those commenters who favored applying the regulation to foreign institutions that do not have offices within the U.S. suggested that an expanded scope would provide additional protections to consumers and would eliminate what they perceive to be a competitive disadvantage of domestic institutions. While the Agencies support consistent protections for consumers regardless of the entity from whom a financial product or service is obtained, at this stage the Agencies do not believe that it is

appropriate to attempt to apply the rule to offshore offices of financial institutions.

Several comments suggested that the rule should not apply to entities that must comply with regulations issued by the Department of Health and Human Services (HHS) that implement the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[4] Given the broad definition of "financial institution" under the GLB Act, certain entities, such as health insurers, are subject to these privacy rules as well as rules promulgated under HIPAA regarding the appropriate handling of protected health information. Accordingly, financial institutions may be covered both by this privacy rule and by the regulations promulgated by HHS under the authority of sections 262 and 264 of HIPAA once those regulations are finalized. Based on the proposed HIPAA rules, it appears likely that there will be areas of overlap between the HIPAA and financial privacy rules. For instance, under the proposed HIPAA regulations, consumers must provide affirmative authorization before a covered institution may disclose medical information in certain instances whereas under the financial privacy rules, institutions need only provide consumers with the opportunity to opt out of disclosures. In this case, the Agencies anticipate that compliance with the affirmative authorization requirement, consistent with the procedures required under HIPAA, would satisfy the opt out requirement under the financial privacy rules. After HHS publishes its final rules, the Agencies will consult with HHS to avoid the imposition of duplicative or inconsistent requirements.

§ __.2 Rule of construction.

Proposed § __.2 of the rules set out a rule of construction intended to clarify the effect of the

---

[4] These proposed regulations were published for comment at 64 FR 59918 (Nov. 3, 1999).

examples used in the rules. As noted in the proposal, these examples are not intended to be exhaustive; rather, they are intended to provide guidance about how the rules would apply in specific situations.

Commenters generally agreed that examples are helpful in clarifying how the rule will work in specific circumstances and suggested that the Agencies should include more examples. Many commenters requested the Agencies to provide examples of model disclosures. Commenters also generally agreed that it is useful to state that the list of examples is not intended to be exhaustive, and that compliance with one of the examples would be deemed compliance with the regulation. A few commenters suggested that the regulation state that a financial institution is not obligated to comply with an example but has the latitude to comply with the general rules in other ways. Others stated that the examples ought to be identical in each privacy regulation adopted by the Agencies, the FTC, NCUA, and SEC.

The Agencies believe that more examples would be helpful, and have included additional examples in appropriate places throughout the rule. The Agencies also have provided sample clauses in Appendix A to each Agency's rule to aid financial institutions in their drafting of privacy notices. The sample clauses are provided to illustrate the level of detail the Agencies believe is appropriate. The Agencies caution financial institutions against relying on the sample disclosures without determining the relevance or appropriateness of the disclosure for their operations. The Agencies have used statutory terms, such as "nonpublic personal information" and "nonaffiliated third parties," in the sample clauses to convey generally the subject of the clauses. However, a financial institution that uses these terms must provide sufficient information to enable consumers to understand what these terms mean in the context of the institution's notices. Moreover, the Agencies note that, in providing the sample disclosures, the

Agencies are addressing solely the level of detail required and are not attempting to provide guidance on issues such as type size, margin width, and so on.

The Agencies have not added a statement in the final rule regarding a financial institution's ability to comply with the rule in ways other than as suggested in the examples, but instead retain the statement that the examples are not exclusive. The rule also states that compliance with the examples will constitute compliance with the rule. The Agencies believe that, when read together, these provisions give financial institutions sufficient flexibility to comply with the regulation but also sufficient guidance about the use of examples.

The Agencies note that an example that mentions a particular activity does not, by itself, authorize a financial institution to engage in that activity. Any such authority must have a different source.

§ __.3 Definitions.

a. Affiliate. The proposal adopted the definition of "affiliate" that is used in section 509(6) of the GLB Act. An affiliation exists 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.

The Agencies received comparatively few comments in response to this definition. One commenter requested that the final rule state that a bank service company will be deemed to be an affiliate of every bank that has an interest in it. The Agencies have declined to adopt this suggestion. If the relationship between a financial institution and a bank service company satisfies the test for affiliation set out in the statute and regulation, then an affiliation exists.

In light of the comparatively few comments received and the nature of those comments, the

Agencies adopt the definition of "affiliate" as proposed.

b. Clear and conspicuous. Under the proposed rules, various notices must be "clear and conspicuous." The proposed rules defined this term to mean that the notice must be reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. The proposal did not mandate the use of any particular technique for making the notices clear and conspicuous, but provided examples of how a notice may be made clear and conspicuous. As noted in the preamble to the proposed rule, each financial institution retains the flexibility to decide for itself how best to comply with this requirement.

The Agencies received a large number of comments on this proposed definition. Several commenters favored adopting the definition as proposed, with some of these advocating that the final rule add a requirement that disclosures be on a separate piece of paper in order to ensure that they will be conspicuous. Others stated that the definition was unnecessary, given the experience financial institutions have in complying with requirements that disclosures mandated by other laws be clear and conspicuous. Several commenters made the related point that the rule proposed is inconsistent with requirements in other consumer protection regulations such as Reg. Z and the Truth in Savings regulation (Regulation DD, 12 CFR part 230), which require only that a disclosure be reasonably understandable. Many of these commenters expressed concern that the examples would invite litigation because of ambiguities inherent in terms used in the examples in the proposed rule such as "ample line spacing," "wide margins," and "explanations ... subject to different interpretations." A few commenters questioned how the requirement would work in a document that contains several disclosures that each must be clearly and conspicuously disclosed, while others raised questions about how a disclosure may

be clear and conspicuous on a website. These comments are addressed below.

New standard for "clear and conspicuous." The Agencies recognize that the proposed definition develops the concept of "clear and conspicuous" beyond what is currently understood by the term. However, the Agencies added the phrase "designed to call attention to the nature and significance of the information contained" to provide meaning to the term "conspicuous." The Agencies believe that this standard, when coupled with the existing standard requiring that a disclosure be readily understandable, likely will result in notices to consumers that communicate effectively the information needed by consumers to make an informed choice about the privacy of their information, including whether to transact business with a financial institution.

The standard for clear and conspicuous adopted by the Agencies in this rulemaking applies solely to disclosures required under the privacy rules. Disclosures governed by other rules requiring clear and conspicuous disclosures (such as Reg. Z) are beyond the scope of this rulemaking.

Examples of "clear and conspicuous." The Agencies recognize that many of the examples are imprecise. The Agencies believe, however, that more prescriptive examples, while perhaps easier to conform to, likely would result in requirements that would be inappropriate in a given circumstance. To avoid this result, the examples provide generally applicable guidance about ways in which a financial institution may make a disclosure clear and conspicuous. The Agencies note that the examples of how to make a disclosure clear and conspicuous are not mandatory. A financial institution must decide for itself how best to comply with the general rule, and may use techniques not listed in the examples. To address concerns about the imprecision of the examples, the Agencies have incorporated several of the commenters' suggestions in the final rule for ways to make the guidance more helpful.

Combination of several "clear and conspicuous" notices. A document may combine several disclosures that each must be clear and conspicuous. The final rule provides an example, in § __.3(b)(2)(ii)(E), of how a financial institution may make disclosures conspicuous, including disclosures on a combined notice. In order to avoid the potential conflicts envisioned by several commenters between two different rules requiring that different sets of disclosures each be provided clearly and conspicuously, the final rule does not mandate precise specifications for how various disclosures must be presented.

Because the Agencies believe that privacy disclosures may be clear and conspicuous when contained in a document containing other disclosures, the rule does not mandate that disclosures be provided on a separate piece of paper. Such a requirement is not necessary and would significantly increase the burden on financial institutions.

Disclosures on web pages. Several commenters requested guidance on how they may clearly and conspicuously disclose privacy-related information on their Internet sites. The Agencies recognize that disclosures over the Internet present some issues that will not arise in paper-based disclosures. There may be web pages within a financial institution's website that consumers may view in a different order each time they access the site, aided by hypertext links. Depending on the customer hardware and software used to access the Internet, some web pages may require consumers to scroll down to view the entire page. To address these issues, the Agencies have included a statement in the example in § __.3(b)(2)(iii) concerning Internet disclosures informing financial institutions that they may comply with the rule if they use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks,

or sound) do not distract attention from the notice. In addition, a financial institution is to place either a notice or a conspicuous link on a page frequently accessed by consumers, such as a home page or a page on which transactions are conducted.

Given current technology, there are a range of approaches a financial institution could take to comply with the rule. For example, a financial institution could use a dialog box that pops up to provide the disclosure before a consumer provides information to the institution. Another approach would be a simple, clearly labeled graphic located near the top of the page or in close proximity to the financial institution's logo, directing the customer, through a hypertext link or hotlink, to the privacy disclosures on a separate web page.

For the reasons advanced above, the Agencies have adopted the definition of "clear and conspicuous," with the changes previously described and with certain other changes intended to make the definition easier to read.

c. Collect. The statute requires a financial institution to include in its initial and annual notices a disclosure of the categories of nonpublic personal information that the institution collects. The proposal defined "collect" to mean obtaining any information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information. This definition was included to provide guidance about the information that a financial institution must include in its notices and to clarify that the obligations arise regardless of whether the financial institution obtains the information from a consumer or from some other source.

Commenters suggested that the final rule treat information that is not organized and retrievable in an automated fashion as not "collected." This approach would exclude separate documents not

included in a file. The Agencies disagree that information should not be deemed to be collected simply because it is not retrievable in an automated fashion. The Agencies believe that the method of retrieval is irrelevant to whether information should be protected under the rule. The Agencies agree, however, that the scope of the regulation should be refined, and have changed the definition of "collect" by using language taken from the Privacy Act of 1974 (5 U.S.C. 552a). By drawing on an existing standard, the final rule will thereby reduce burden that otherwise would result from having to comply with conflicting rules governing the collection of information.

Other commenters requested that the rule clarify that information that is received by a financial institution but then immediately passed along without maintaining a copy of the information is not "collected" as this term is used in the final rule. The Agencies believe that merely receiving information without maintaining it would not be "collecting" the information. The final rule reflects this by stating that the information must be organized or retrievable by the financial institution. Otherwise, the definition of "collect" is adopted as proposed.

d. Company. The proposal defined "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.

The Agencies received no substantive comments on this proposed definition. Accordingly, the Agencies adopt the definition of "company" as proposed.

e. Consumer. The GLB Act distinguishes "consumers" from "customers" for purposes of the notice requirements imposed by the Act. 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 purposes other than as permitted by section 502(e) of the statute (as implemented by §§ __.14 and __.15 of the final rule). By contrast, a financial institution must give all "customers" a notice of the institution's privacy policy at the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship.

The proposal defined "consumer" to mean an individual (and his or her legal representative) who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes. Because "financial product or service" is defined to include the evaluation by a financial institution of an application to obtain a financial product or service (see further discussion of this point, below) a person becomes a consumer even if the application is denied or withdrawn. An individual also would 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 Agencies received a large number of comments on this proposed definition, raising questions about how the definition would apply in a variety of situations. These comments are addressed below.

Distinction between "consumer" and "customer." While many agreed with the distinction drawn in the proposal between "consumer" and "customer," a few commenters suggested that no distinction between "consumer" and "customer" should be made, given that, in these commenters' views, the statute appears to use the terms interchangeably. The Agencies believe, however, that the distinction was deliberate and that the rule should implement it accordingly. A plain reading of the statute supports the conclusion that Congress created one set of protections (i.e., a financial institution's privacy policy and opt out notice, and the right to opt out if a financial institution intends to disclose

nonpublic personal information to nonaffiliated third parties) for anyone who obtains a financial product or service and an additional set of protections (i.e., the initial notices at the time of establishing a customer relationship and annual notices thereafter) for anyone who establishes a relationship of a more lasting nature than an isolated transaction with a financial institution. Thus, the statute tailors the notice requirements to the type of relationship an individual has with a financial institution. This distinction is preserved in the final rule.

Applicants as consumers. Many of the comments on the proposed definition of "consumer" disagreed that someone should be deemed a consumer of a financial institution simply by virtue of the institution evaluating an application. These commenters maintained that the individual has not obtained a financial product or service, as is required by the statutory definition of "consumer." The Agencies remain of the view, however, that it is consistent with both the spirit and the letter of the GLB Act to consider an individual as having obtained a financial product or service when a financial institution evaluates information provided to the financial institution for the purpose of the individual obtaining some other financial product or service. Financial institutions frequently provide a range of services in connection with the delivery of a financial product. Included within these will be the evaluation by the financial institution of information provided by an individual. In certain instances, such as when an individual is shopping for the best rate on a mortgage loan or the lowest premium for an insurance policy, that evaluation may be the sole financial product or service obtained. In other instances, the evaluation may be one of several services provided that lead up to the eventual establishment of a customer relationship. In either case, the individual will have obtained a financial product or service from the financial institution when the financial institution evaluates the information and provides the

individual the information sought.

In addition to being consistent with the language of the statute, the proposed definition of "consumer" is consistent with one of the primary purposes of Title V of GLB Act, namely, to enable an individual to limit the sharing of nonpublic personal information by a financial institution with a nonaffiliated third party. The information provided by a person to a financial institution before a customer relationship is established is likely to contain the types of information that the statute is designed to protect. This information is no less deserving of protection simply because an application is denied or withdrawn. For these reasons, the Agencies have retained within the definition of "consumer" individuals whose applications are evaluated by a financial institution. See § __.3(e)(2)(i).

Loan sales. Several commenters requested clarification of whether an individual becomes a consumer in various other scenarios involving loans. Commenters posited a wide variety of examples, which, if each were to be addressed specifically in the rule, would require a final rule of enormous complexity and detail. The Agencies believe that a rule setting forth a general principle that is flexible enough to be applied in the array of loan transactions posited by the commenters is more appropriate.

Towards this end, the Agencies have stated in the final rule, at § __.3(e)(2)(iv), that a person will be a consumer of any entity that holds ownership or servicing rights to an individual's loan. (The Agencies note that such a person may not be a customer, however; see explanation of how the definition "customer" will be applied in the loan context, in the discussion of the definition of "customer" below. See also §§ __.4(c)(2) and __.4(c)(3)(ii) for further discussion concerning when a borrower establishes a customer relationship in the context of a loan sale.) The Agencies believe that financial institutions that own or service a loan are providing a financial product or service to the individual

borrower in question. In some cases, the product or service is the funding of the loan, directly or indirectly. In other cases, the product or service is the processing of payments, sending account-related notices, responding to consumer questions and complaints about the handling of the account, and so on. The final rule defines "consumer" in a way that covers individuals receiving financial products or services in each of these situations.

Agents of financial institutions. Several commenters agreed with the principle set out in the proposed rule that an individual should not be considered to be a consumer of an entity that is acting as agent for a financial institution. These commenters noted that the financial institution that hires the agent is responsible for that agent's conduct in carrying out the agency responsibilities. The Agencies agree and continue to believe that the financial institution is the entity that has a consumer relationship, even if it uses agents to help it deliver its products or services. Accordingly, the proposed rule retains the rule governing agents, with modifications made to improve its clarity. See § __.3(e)(2)(v).

Legal representative. The Agencies also agree with the suggestion made by several commenters that the definition of "consumer" should clarify that the obligations stemming from a consumer relationship may be satisfied by dealing either with the individual who obtains a financial product or service from a financial institution or that individual's representative. The Agencies do not intend for the rule to require a financial institution to send opt out and initial notices to both the individual and the individual's legal representatives, and have amended the final rule accordingly in § __.3(e)(1).

Trusts. The Agencies received several comments concerning whether an individual who obtains financial services in connection with trusts is a consumer or customer of a financial institution.

Several commenters urged the Agencies to generally exempt a financial institution from the requirements of the rule when it acts as a fiduciary, or, in the alternative, clarify the categories of individuals that are considered to be customers. Commenters proposed, for example, that individuals who are beneficiaries with current interests should be identified as customers, whereas individuals who are only contingent beneficiaries should not be customers. Other commenters stated that when the financial institution serves as trustee of a trust, neither the grantor nor beneficiary is a consumer or customer under the rule. In these commenters' view, the trust itself is the institution's "customer," and, therefore, the rule should not apply to a financial institution when it acts as trustee. These commenters also stated that when a financial institution is a trustee, it serves as a fiduciary and is subject to other obligations to protect the confidentiality of the beneficiaries' information that are more stringent than those under the provisions in the GLB Act. Similarly, these and other commenters claimed that an individual who is a participant in an employee benefit plan administered or advised by a financial institution does not qualify as a consumer or customer. The commenters opined that the plan sponsor, or the plan itself, is the "customer" for the purposes of the proposed rule. These commenters contended that plan participants have no direct relationship with the financial institution and, in any event, the financial institution is authorized to use information that would be covered under the GLB Act only in accordance with the directions of the plan sponsor. The commenters concluded, therefore, that the regulations should specifically exclude individuals who are participants in an employee benefit plan from the definition of customer.

The Agencies believe that the definition of "consumer" in the GLB Act does not squarely resolve whether the beneficiary of a trust is a consumer of the financial institution that is the trustee. The

Agencies agree with the commenters who concluded that, when the financial institution serves as trustee of a trust, neither the grantor nor beneficiary is a consumer or customer under the rule. Instead, the trust itself is the institution's "customer," and therefore, the rule does not apply because the trust is not an individual. The Agencies note that a financial institution that is a trustee assumes obligations as a fiduciary, including the duty to protect the confidentiality of the beneficiaries' information, that are consistent with the purposes of the GLB Act and enforceable under state law. Accordingly, the Agencies have excluded an individual who is a beneficiary of a trust or a plan participant of an employee benefit plan from the definitions of "consumer" and "customer." Nevertheless, the Agencies believe that an individual who selects a financial institution to be a custodian of securities or assets in an IRA is a "consumer" under the GLB Act. The Agencies have included examples in the rule that appropriately illustrate this interpretation of the GLB Act in §§ __.3(e)(2)(vi) - (viii) and § __.3(i)(2)(i)(D).

Requirements arising from consumer relationship. While the proposed and final rules define "consumer" broadly, the Agencies note that this will not result in any additional burden to a financial institution in situations where (a) no customer relationship is established and (b) the institution does not intend to disclose nonpublic personal information about a consumer to nonaffiliated third parties. Under the approach taken in the final rule, a financial institution is under no obligation to provide a consumer with any privacy disclosures unless it intends to disclose the consumer's nonpublic personal information to nonaffiliated third parties outside the exemptions in §§ __.14 and __.15. A financial institution that wants to disclose a consumer's nonpublic personal information to nonaffiliated third parties is not prohibited under the final rule from doing so, if the requisite notices are delivered and

the consumer does not opt out. Thus, as it applies to consumers who are not customers, the rule allows a financial institution to avoid all of the rule's requirements if it chooses to do so. Conversely, if a financial institution determines that the benefits of disclosing consumers' nonpublic personal information to nonaffiliated third parties outweighs the attendant burdens, the financial institution is free to do so, provided it notifies consumers about the disclosure and affords them a reasonable opportunity to opt out. In this way, the rule attempts to strike a balance between protecting an individual's nonpublic personal information and minimizing the burden on a financial institution.

f. Consumer reporting agency. The proposal adopted 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 was used in proposed §§ __.11 and __.13.

The Agencies received no comments suggesting any changes to this definition. Accordingly, the definition is adopted as proposed. It is used in §§ __.6(f), __.12(a), and __.15(a)(5) of the final rule.

g. Control. The proposal defined "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 § __.3(a), above), and would result in financial institutions being considered as affiliates regardless of whether the control is by a company or individual.

The Agencies received few comments in response to this definition. The one substantive suggestion received was to adopt a test focused solely on percent of stock owned in a company so as to avoid the uncertainties arising from a "control in fact" test. The Agencies believe, however, that any test based only on stock ownership is unlikely to be flexible enough to address all situations in which companies are appropriately deemed to be affiliated. Accordingly, the Agencies adopt the definition of

"control" as proposed.

h. Customer. The proposal defined "customer" as any consumer who has a "customer relationship" with a particular financial institution. As is explained more fully in the discussion of § __.4, below, a consumer is a customer of a financial institution when the consumer has a continuing relationship with the institution.

The Agencies received a large number of comments on the definition of "customer" and "customer relationship." Given the interdependence of the two terms, the following analysis of the comments received will address both under the heading "customer relationship."

i. Customer relationship. The proposed rules defined "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.[5] As noted in the proposal, a one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. A consumer would not become a customer simply by repeatedly engaging in isolated transactions that by themselves would be insufficient to establish a customer relationship, such as withdrawing funds at regular intervals from an ATM owned by an institution at which the consumer has no account. The proposal also stated that a consumer would 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. The Agencies received a large number of comments on this definition, as discussed below.

---

[5] As noted in the preamble to the proposed rule, "customer" may be defined differently for purposes of other regulations. See, e.g., 12 CFR 7.4002.

Point at which one becomes a customer. The Agencies received many comments in response to the definitions of "customer" and "customer relationship." Commenters criticized what they considered to be the ill-defined line distinguishing consumers from customers. These commenters stated that the proposed distinction makes it difficult for a financial institution to know when the obligations attendant to a customer relationship arise. Several suggested that the distinction should be based on when a consumer and financial institution enter into a written contract for a financial product or service.

The Agencies recognize that the distinction between consumers and customers will, in some instances, require a financial institution to make a judgment about whether a customer relationship is established. In those cases where an individual engages in a transaction for which it is reasonable to expect no further communication about that transaction from the financial institution (such as ATM transactions, purchases of money orders, or cashing of checks), the individual will not have established a customer relationship as a result of that transaction. In other situations where a consumer typically would receive some measure of continued service following, or in connection with, a transaction (such as would be the case when a consumer opens a deposit account, borrows money, or obtains investment advice), a customer relationship will be established. The Agencies believe that the distinction set out in the proposed rule, as further clarified by the examples in the final rule of when a customer relationship is, and is not, established, provides a sufficiently clear line while retaining flexibility to address less clear-cut situations on a case-by-case basis.

Customer relationship defined by written contract. The Agencies agree with those commenters who consider the execution of a written contract by a consumer and financial institution as

clear evidence that a customer relationship has been established. The proposed rule cited the execution of a written contract as an example of when a customer relationship is established, and the final rule retains that example in § __.4(c)(3)(i)(B). However, a test based solely on whether there is a written contract could inappropriately exclude situations in which an individual is a customer of a financial institution as a result of obtaining, for instance, financial, economic, or investment advisory services from a financial institution. Accordingly, the final rule does not define a customer relationship solely by the execution of a written contract.

Use of "isolated transaction" test. The final rule also does not define the distinction between consumer and customer based solely on whether the transaction is an isolated event. The Agencies used this concept in several examples in the proposed rule to illustrate one of the factors that may go into whether a relationship is of a continuing nature. Several commenters suggested that this approach was insufficiently precise to serve as a workable distinction between consumers and customers. The Agencies agree that the test may not be useful in all instances, but believe that it will help clarify the status of relationships in certain situations. Accordingly, the final rule retains examples in §§ __.3(i)(2)(ii)(A) and (C) that cite the isolated nature of a given transaction as an indication that the transaction in question does not establish a customer relationship.

Purchase of insurance. Other commenters suggested that, in the context of financial institutions that engage in the sale of insurance and that are regulated by the Agencies, the customer should be the policyholder and not the beneficiary. The Agencies agree, and note that the final rule retains the example § __.3(i)(2)(i)(D) of purchasing an insurance product as one situation in which a customer relationship is formed. In this case, the person obtaining a financial product or service from

the financial institution is the person purchasing the policy. The beneficiaries would be recipients of the insurance proceeds, thereby entitling them to the protections afforded consumers.

Sales of loans. As previously noted, several commenters raised questions in the context of loan sales. Many commenters stated that, under the final rule, a person should not be considered a customer of two financial institutions when the originating bank sells the servicing rights. A point consistently made by these commenters was that a borrower would be equally well protected with less risk of confusion if the borrower is deemed to be a customer of only one entity in connection with a loan, with that entity perhaps being the party with whom the borrower communicates about the loan. The Agencies believe that it is appropriate to consider a loan transaction as giving rise to only one customer relationship, with the recognition that this customer relationship may be transferred in connection with a sale of part or all of the loan. In this way, the borrower will not be inundated by privacy notices, many of which might be from subservicers that the borrower did not know had any connection to his or her loan. The Agencies note, however, that a customer will remain a consumer of the entity that transfers the servicing rights, as well as a consumer of any other entity that holds an interest in the loan.

In order to satisfy the statutory requirement that a customer receive an annual notice from a financial institution until that relationship terminates, the final rule provides that the borrower must be deemed to have a customer relationship with at least one of the entities that hold an interest in the loan. In the case of a financial institution that makes a loan, retains it in its portfolio, and provides servicing for the loan, the borrower clearly would have a customer relationship with that institution. Less clear, however, are situations in which servicing is sold or investors purchase a partial interest in a loan. The

Agencies have adopted an approach designed to ensure that a customer receives annual notices for the duration of the customer relationship from the most appropriate financial institution.

Under the final rule as stated in § __.3(i)(2)(i)(B), a customer relationship will be established as a general rule with the financial institution that makes a loan to an individual. This customer relationship then will attach to the entity providing servicing. Thus, if the originating lender retains the servicing, it will continue to have a customer relationship with the borrower and will be obligated to provide annual notices for the duration of the customer relationship. If the servicing is sold, then the purchaser of the servicing rights will establish a customer relationship (and the originating lender will have a consumer relationship with the borrower). See § __.3(i)(2)(ii)(B). In this way, the borrower will be entitled to receive an initial notice and annual notices from the loan servicer, but will not be inundated by initial and annual notices from entities that hold interests in the loan but are unknown to the consumer.

Mortgage brokers. Several commenters suggested that the use of a mortgage broker should not create a customer relationship. The Agencies disagree. A relationship between a mortgage broker and a consumer is more than an isolated transaction, given that the mortgage broker is likely to provide many services for a consumer, such as analyzing financial information, performing credit checks, negotiating with other financial institutions on the consumer's behalf, and assisting with loan closings. In light of the similarities between the services provided by a mortgage broker and those provided by, for instance, an insured depository institution that makes a mortgage loan, the Agencies believe it is appropriate to consider a mortgage broker to be a financial institution that establishes a customer relationship when the broker enters into an agreement or understanding with a consumer whereby the broker undertakes to arrange or broker a home mortgage loan for the consumer. The final rule reflects

this in § __.3(i)(2)(i)(F).

Trusts. The final rule adds an example in § __.3(i)(2)(i)(E) to clarify that an individual will be deemed to establish a customer relationship when a bank acts as a custodian for securities or assets in an IRA. This example is consistent with the explanation set out above in the discussion of "consumer" concerning trusts.

j. Federal functional regulator. The proposal sought comment on a definition of "government regulator" that included 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 was used in the exception set out in proposed § __.11(a)(4) for disclosures to law enforcement agencies, "including government regulators."

The few comments that were received on this definition suggested that it be expanded to include additional governmental entities. The Agencies note that, for purposes of the privacy rule, this term is relevant only in the discussion of when a financial institution may disclose information to a law enforcement agency. The exception as stated in the statute uses the term "federal functional regulator" (see section 502(e)(5)), which term is defined in the statute at section 509(2) and also includes the Secretary of the Treasury for purposes of the exception permitting disclosures to law enforcement agencies. The Agencies have decided that it is appropriate simply to use the term that is used in the statute and adopt its definition.

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

1843(k)). The proposal exempted from the definition of "financial institution" those entities specifically excluded by the GLB Act.

Commenters suggested that the final rule contain several exclusions to this definition, including those for securitization trusts, debt buyers, and credit bureaus. The Agencies have not included these exceptions in the final rule, in part because the Agencies believe that it is inappropriate to exclude many of the activities suggested by commenters and in part because the objective of the suggested exclusions can be achieved in other ways. Even if an entity is a financial institution as that term is used in the GLB Act, it will not have any disclosure responsibilities under the Act or this rule if it does not provide a financial product or service to a consumer. In most of the situations posited by the commenters, the entity in question will not meet that test and, therefore, will fall outside the scope of the rule with respect to privacy disclosures.[6]

For the reasons discussed above, the Agencies adopt the definition of "financial institution" as proposed.

l. Financial product or service. The proposal defined "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), was not included in the proposed definition of "financial product or service." The proposal's definition included

[6] However, these entities will be subject to the limits on redisclosures under § __.11 with respect to any nonpublic personal information they receive from a nonaffiliated financial institution that has disclosure obligations under this rule.

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 included the distribution of information about a consumer for the purpose of assisting the consumer in obtaining a financial product or service.

The most frequently expressed comment in response to this proposed definition was that the evaluation of application information should not be considered a financial product or service. For the reasons advanced above in the discussion of the definition of "consumer," the Agencies continue to believe that it is appropriate to retain evaluation activity within the scope of financial product or service covered by the rule. It is one of many financial services provided by financial institutions. Moreover, a consumer is likely to provide the type of the nonpublic personal information that the statute is designed to protect in the course of obtaining the financial institution's evaluation. Accordingly, the final rule adopts the definition of "financial product or service" as proposed.

m. Nonaffiliated third party. The proposal defined "nonaffiliated third party" as any person (which includes natural persons as well as corporate entities) except (1) an affiliate of a financial institution and (2) a joint employee of a financial institution and a third party. The proposal clarified the circumstances under which a company that is controlled by a financial institution pursuant to that institution's merchant banking activities or insurance company activities would be a "nonaffiliated third party" of that financial institution.

The Agencies received very few comments in response to this proposed definition. One commenter requested that the final rule state that a disclosure of information to someone who is serving as a joint employee of two financial institutions should be deemed to have been disclosed to both

financial institutions. The Agencies disagree with this result. Instead, the Agencies believe it is appropriate to deem the information to have been given to the financial institution that is providing the financial product or service in question. Thus, for instance, if an employee of an insured depository institution is a dual employee with a securities firm, information received by that person in connection with a securities transaction conducted with the securities firm would be deemed to have been received by the securities firm.

In light of the comments received, the Agencies adopt the definition of "nonaffiliated third party" as proposed.

n. Nonpublic personal information. Section 509(4) of the GLB Act defines "nonpublic personal information" to mean "personally identifiable financial information" that is provided by a consumer to a financial institution, results from any transaction with the consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. It also includes any "list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information." The statute excludes publicly available information (unless provided as part of the list, description or other grouping described above), as well as a list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using nonpublic personal information. The statute does not define either "personally identifiable financial information" or "publicly available information."

The proposed rules implemented this provision of the GLB Act by restating the categories of information described above. The proposed rules presented two alternative approaches to identifying

what information would be regarded as publicly available (and therefore, as a general rule, outside the definition of "nonpublic personal information"). Alternative A deemed information as publicly available only if a financial institution actually obtained the information from a public source while Alternative B treated information as publicly available if a financial institution could obtain it from such a source. Both Alternatives A and B included within the definition of “nonpublic personal information” publicly available information that is provided as part of a list, description, or other grouping of consumers.

Commenters favoring Alternative A noted that it provided the greatest protection for consumers by treating anything the consumer gives to a financial institution to obtain a financial product or service as nonpublic personal information. Under Alternative A, this protection would be lost only if a financial institution actually obtained the information from a public source. These commenters also preferred the bright-line distinction drawn by treating as nonpublic personal information any information given by a consumer to obtain a financial product or service or information that results from transactions between a financial institution and a consumer. However, the majority of those commenting on this issue favored Alternative B, noting that this alternative was consistent with the statute and would be far less burdensome on financial institutions. These commenters suggested that a requirement that the information actually be obtained from a public source would impose needless burden on financial institutions (by requiring, for instance, that a financial institution “tag” information they obtained from public records) and is not required by the statute.

The final rule adopts an approach that the Agencies believe incorporates the benefits of both alternatives. Under the final rule, information will be deemed to be “publicly available” and therefore excluded from the definition of “nonpublic personal information” if a financial institution has a reasonable

basis to believe that the information is lawfully made available to the general public from one of the three categories of sources listed in the rule. See § __.3(p)(1). The final rule states that a financial institution will have a "reasonable basis" for believing that information is lawfully made available if it has taken steps to determine that the information is of the type that is available to the general public and, if an individual could direct that the information not be made available to the general public, whether the individual has done so. In this way, a financial institution will be able to avoid the burden of having to actually obtain information from a public source, but will not be free simply to assume that information is publicly available without some reasonable basis for that belief. The final rule cites, as an example of information a financial institution might reasonably believe to be publicly available, the fact that someone has a loan that is secured by a mortgage in jurisdictions where mortgages are recorded. See § __.3(p)(3)(iii)(1). The rule also states that a financial institution will have a reasonable basis to believe that a telephone number is publicly available if the institution either located the number in a telephone book or was informed by the consumer that the number is not unlisted. See § __.3(p)(3)(iii)(2).

This approach is based on the underlying principle that, if a consumer has some measure of control over the public availability of his or her information, a financial institution should not automatically assume that the information is in fact publicly available. In the case of a mortgage in most jurisdictions, the borrower has no choice about whether the lender will make the mortgage a matter of public record; a lender must do so in order to protect its security interest. In the case of a telephone number, a person may request that his or her number be unlisted. Thus, in evaluating whether it is reasonable to believe that information is publicly available, a financial institution should consider whether the information is of a type that a consumer could keep from being a matter of public record.

To implement the complex definition of "nonpublic personal information" that is provided in the statute, the final rule adopts a definition that consists, generally speaking, of (1) personally identifiable financial information, plus (2) a consumer list (and publicly available information pertaining to the consumers) that is derived using only personally identifiable financial information that is not publicly available. From that body of information, the final rule excludes publicly available information (except as noted above) and any consumer list that is derived without using personally identifiable financial information that is not publicly available. See §§ __.3(n)(1) and (2). Examples are provided in § __.3(n)(3) to illustrate how this definition applies in the context of consumer lists.

o. Personally identifiable financial information. The proposed rules defined “personally identifiable financial information” to include information that a consumer provides a financial institution in order to obtain a financial product or service, information resulting from any transaction between the consumer and the financial institution involving a financial product or service, and information about a consumer a financial institution otherwise obtains in connection with providing a financial product or service to the consumer. The proposed rule also treated the fact that someone is a customer of a financial institution as personally identifiable financial information. In essence, the proposed rules treated any personally identifiable information as financial if it was obtained by a financial institution in connection with providing a financial product or service to a consumer. The Agencies noted in the preamble to the proposed rule that this interpretation may result in certain information being covered by the rules that may not be considered intrinsically financial, such as health status.

The Agencies received a large number of comments in response to this definition, most of which stated that the definition inappropriately included certain identifying information that is not financial, such

as name, address, and telephone number. Many others maintained that "personally identifiable financial information" should not include the fact that someone is a customer of a financial institution. These commenters typically noted that many customer relationships are matters of public record (such as would be the case, for instance, anytime a transaction results in the recordation of a security interest) while other customer relationships are matters of public knowledge (because consumers frequently disclose the relationships by writing checks, using credit cards, and so on). Many commenters stated that aggregate data about a financial institution's customers that lack personal identifiers should not be considered personally identifiable financial information.

Treatment of identifying information as financial. The Agencies continue to believe that it is appropriate to treat any information as financial information if it is requested by a financial institution for the purpose of providing a financial product or service. The Agencies also believe this approach is consistent with the broad definition of "financial institution" used in the statute, which encompasses a large number of entities (such as travel agencies, insurance companies, and data processors) that engage in activities not traditionally considered financial. As a consequence of that definition, the range of information that has a bearing on the terms and availability of a financial product or service or that is used by a financial institution in connection with providing a financial product or service is extremely broad and may include, for instance, medical information and other sorts of information that might not be thought of as financial.

The Agencies are sensitive to the concern expressed by many commenters, including several hundred private investigators, about the need for ready access to identifying information to locate people attempting to evade their financial obligations. These commenters consistently suggested that

names, addresses, and telephone numbers should not be treated as financial information. However, financial institutions rely on a broad range of information, including information such as addresses and telephone numbers, when providing financial products or services. Location information is used by financial institutions to provide a wide variety of financial services, from the sending of checking account statements to the disbursing of funds to a consumer. Other information, such as the maiden name of a consumer's mother often will be used by a financial institution to verify the consumer's identity. The Agencies concluded that it would be inappropriate to carve out certain items of information simply because a particular financial institution might not rely on those items when providing a particular financial product or service.

The Agencies note that names, addresses, and telephone numbers, if publicly available, will not be subject to the opt out provisions of the statute unless that information is "derivative information" (i.e., information that is part of a list, description, or other grouping of consumers that is derived from personally identifiable financial information that is not publicly available). Thus, in instances involving specific requests about individuals, a financial institution still may disclose information about the individual that the institution reasonably believes to be publicly available, provided that in so doing the institution does not disclose the existence of a customer relationship that is not a matter of public record. Moreover, in instances when a consumer does not opt out, a financial institution may disclose any nonpublic personal information to a nonaffiliated third party provided that the disclosure is consistent with the institution's opt out and privacy notices.

Customer relationship as "personally identifiable financial information." The Agencies disagree with those commenters who maintain that customer relationships should not be considered to

be personally identifiable financial information. Clearly, information that a particular person has a customer relationship identifies that person, and thus is personally identifiable. The Agencies believe that this information also is financial, because it communicates that the person in question has a transaction involving a financial product or service with a financial institution. While this information could in certain cases be a matter of public record, that does not change the analysis of whether the information is personally identifiable financial information.

Changes made to the definition. The final rule makes various stylistic changes to the definition that are intended to make it easier to read and understand. In addition, the final rule adds to the examples of information covered by the rule any information that the institution collects through an information collecting device from a web server, often referred to as a "cookie." See § __.3(o)(2)(F). This illustrates one of the various means by which a financial institution may "otherwise obtain" information about a consumer in connection with providing a financial product or service to that consumer.

The final rule also includes, as a negative example in § __.3(o)(2)(ii)(B), a statement that aggregate information or blind data lacking personal identifiers is not covered by the definition of "personally identifiable financial information." The Agencies agree with those commenters who opined that such data, by definition, do not identify any individual.

p. Publicly available information. The proposal defined "publicly available information" to include information that is lawfully available to the public from official public records (such as real estate recordations or security interest filings), information from widely distributed media (such as a telephone book, television or radio program, or newspaper), and information that is required to be disclosed to

the general public by Federal, State, or local law (such as securities disclosure documents). The proposed rules stated that publicly available information from widely distributed media would include information from an Internet site that is available to the general public without requiring a password or similar restriction.

As previously explained in the discussion of "nonpublic personal information," the proposed rules invited comment on two versions of the definition of "publicly available information." The Agencies have adopted an approach in the final rule that they believe more closely tracks the statute while providing much of the benefit provided under Alternative A.

Several commenters questioned the appropriateness of excluding information from the definition of "publicly available information" if a person who seeks to obtain the information over the Internet must have a password or comply with a similar restriction. These commenters made the point that many Internet sites are available to a large number of people, each of whom need a user name and identification number to access the sites. Several of these commenters suggested that it is more appropriate to focus on whether the information was lawfully placed on the Internet.

The Agencies agree with these comments, and have amended the final rule to remove the reference to passwords or similar restrictions from the example of the Internet as a "widely distributed" medium of communication. In its place, the Agencies have substituted a standard that the information be available on an unrestricted basis, and then stated in the rule that a site is not restricted merely because an Internet service provider or a site operator requires a fee or password as long as access is otherwise available to the general public. The traditional use of passwords is to confine the access of individual customers to specific, individual information. However, website operators, in particular, may

require user identifications and passwords as a method of tracking access rather than restricting access to the information available through the website. Fees may be levied to enhance the revenue of the Internet service provider or site operator rather than restrict access. Therefore, the Agencies believe that the definition of "widely distributed media" should properly focus on whether the information is lawfully available to the general public, rather than on the type of medium from which information is obtained.

The Agencies note that the concept of information being lawfully obtained was included in the proposal, and is retained in the final rule. Thus, information unlawfully obtained will not be deemed to be publicly available notwithstanding that it may be available to the general public through widely distributed media.

To help understand how "nonpublic personal information," "personally identifiable financial information," and "publicly available information" will work under the final rule, the following example is offered. Assume that Mary provides her bank with various information in order to obtain a mortgage loan and to open a deposit account. Under the final rule, all of this information would be personally identifiable financial information. Once Mary establishes the customer relationships she seeks, the fact that Mary is a mortgage loan customer and a deposit accountholder at the bank also would be personally identifiable financial information.

It may be that certain information provided by Mary, such as her name and address, is publicly available. If the bank has a reasonable basis to believe that this information is publicly available, and if the information was included on a list of all of the bank's mortgage loan customers, then her name and address would fall outside the definition of "nonpublic personal information" in those jurisdictions where

mortgages are a matter of public record. However, Mary's name and address would be protected as nonpublic personal information if the bank wanted to include those items on a list of its deposit accountholders. The difference in treatment stems from the distinction drawn in the statute between lists prepared using publicly available information (as would be the case in the mortgage loan hypothetical) and lists prepared using information that is not publicly available (as would be the case in the deposit account hypothetical).

The Agencies recognize the complexity of this approach, but believe that it is mandated by the way the statute defines "nonpublic personal information." It also is consistent with the fact that certain relationships are matters of public record, and, therefore, arguably deserving of less protection from disclosure.

q. You. Several Agencies used the pronoun "you" to refer to entities within their primary jurisdiction in the proposal and defined "you" to mean those entities.[7]

The Agencies received very few comments in response to this definition. While one commenter preferred the term "bank" to "you," those Agencies using the term "you" believe that it makes the rule easier to read and have, therefore, adopted the definition substantially as proposed. The Board has revised its definition of "you" to clarify that insurance subsidiaries of the financial institutions within its primary jurisdiction are not covered.

§ __.4 Initial privacy notice to consumers required.

The GLB Act requires a financial institution to provide an initial notice of its privacy policies and

---

[7] The OCC used the term "bank" instead of "you" in its regulation.

practices in two circumstances. For customers, the notice must be provided at the time of establishing a customer relationship. For consumers who are not customers, the notice must be provided prior to disclosing nonpublic personal information about the consumer to a nonaffiliated third party.

The proposed rule implemented these requirements by mandating that a financial institution provide the initial notice to an individual prior to the time a customer relationship is established and the opt out notice prior to disclosing nonpublic personal information to nonaffiliated third parties. These disclosures were required under the rule to be clear and conspicuous and to accurately reflect the institution's privacy policies and practices. The proposal also set out rules governing when a customer relationship is established and how a financial institution is to provide notice.

The Agencies received many comments raising concerns about a large number of issues arising under proposed § __.4. Most of the comments raised questions about the time by which initial notices must be provided, whether new notices are required for each new financial product or service obtained by a customer, the point at which a customer relationship is established, and how initial notices may be provided.

Providing initial notices "prior to" time customer relationship is established. Many commenters stated that, because the statute requires only that the initial notice be provided "at the time of establishing a customer relationship," the regulation should not require that the notice be provided "prior to" the point at which a customer relationship is established. These commenters were concerned that the rule could be interpreted as requiring a financial institution to provide disclosures at a point different from when they must provide other federally mandated consumer disclosures during the process of establishing a customer relationship.

In response to these comments, the Agencies have clarified the timing for providing initial notices. The final rule states that, as a general rule, the initial notice must be given not later than the time when a financial institution establishes a customer relationship. See § __.4(a)(1). As stated in the preamble to the proposed rule, the initial 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 TILA. This approach, like the approach taken in the proposed rule, strikes 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 burden on financial institutions that may otherwise result if the final rule were to require financial institutions to provide consumers with a series of notices at different times in a transaction.

Providing notices after customer relationship is established. Several commenters stated that the rule should provide financial institutions with the flexibility to deliver the initial notice after the customer relationship is established under certain circumstances. These commenters posited several situations in which a customer relationship is established without face-to-face contact between the consumer and financial institution. The commenters stated that delivery of the initial notice before the customer relationship is established in these situations would be impractical, and a requirement along those lines would have a significant adverse effect on the ability to provide a financial product or service to a consumer as quickly as the consumer desires.

The Agencies believe that it is appropriate for financial institutions to have flexibility in certain circumstances to provide the initial notice at a point after the customer relationship is established. To accommodate the wider range of situations presented by the commenters, the Agencies have modified

the examples set out in the proposal of when a subsequent delivery of the initial notice is appropriate so that they now are more broadly applicable. As stated in the final rule in § __.4(e), a financial institution may provide the initial notice within a reasonable time after establishing a customer relationship in two instances. First, notice may be provided after the fact if the establishment of the customer relationship is not at the customer's election. See § __.4(e)(1)(i). This might occur, for instance, when a deposit account is sold. Second, a notice may be sent after establishing a customer relationship when to do otherwise would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time. See § __.4(e)(1)(ii). An example of this would be when a transaction is conducted over the telephone and the customer desires prompt delivery of the item purchased. Another example of when this might occur is when a bank establishes a customer relationship with an individual under a student loan program as described in the final rule where loan proceeds are disbursed promptly without prior communication between the bank and the customer.

The Agencies note that in most situations, and particularly in situations involving the establishment of a customer relationship in person, a financial institution should give the initial notice at a point when the consumer still has a meaningful choice about whether to enter into the customer relationship. The exceptions listed in the examples, while not exhaustive, are intended to illustrate the less frequent situations when delivery either would pose a significant impediment to the conduct of a routine business practice or the consumer agrees to receive the notice later in order to obtain a financial product or service immediately.

In circumstances when it is appropriate to deliver an initial notice after the customer relationship is established, a financial institution should deliver the notice within a reasonable time thereafter. Several

commenters requested that the final rule specify precisely how many days a financial institution has in which to deliver the notice under these circumstances. However, the Agencies believe that a rule prescribing the maximum number of days would be inappropriate because (a) the circumstances of when an after-the-fact notice is appropriate are likely to vary significantly, and (b) a rule that attempts to accommodate every circumstance is likely to provide more time than is appropriate in many instances. Thus, rather than establish a rule that the Agencies believe may be viewed as applicable in all circumstances, the Agencies have elected to retain the more general rule as set out in the proposal in § __.4(e)(1).

As the Agencies noted in the preamble to the proposed rule, nothing in the rule is intended to discourage a financial institution from providing an individual with a privacy notice at an earlier point in the relationship 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.

New notices not required for each new financial product or service. Several commenters asked whether a new initial notice is required every time a consumer obtains a financial product or service from that financial institution. These commenters suggested that a consumer would not materially benefit from repeated disclosures of the same information, and that requiring additional initial notices to be provided to the same consumer would be burdensome on financial institutions.

The Agencies agree that it would be burdensome with little corresponding benefit to the consumer to require a financial institution to provide the same consumer with additional copies of its initial notice every time the consumer obtains a financial product or service. Accordingly, the final rule states, in § __.4(d), that a financial institution will satisfy the notice requirements when an existing

customer obtains a new financial product or service if the institution's initial, revised, or annual notice (as appropriate) is accurate with respect to the new financial product or service.

Joint accountholders. The majority of comments on how to provide notice suggested that the final rule state that a financial institution is not obligated to provide more than one notice to joint accountholders. Several of these commenters noted that disclosure obligations arising from joint accounts are well settled under other rules, such as the regulations implementing the Equal Credit Opportunity Act (Regulation B, 12 CFR part 202,) and TILA. Commenters noted that under both Reg. B and Reg. Z, a financial institution is permitted to give only one notice. The authorities cited include requirements that the financial institution give disclosures, as appropriate, to the "primary applicant" if this is readily apparent (in the case of Reg. B; see 12 CFR 202.9(f)) or to a person "primarily liable on the account" (in the case of Reg. Z; see 12 CFR 226.5(b)).

The Agencies agree that a financial institution should be allowed to provide initial notices in a manner consistent with other disclosure obligations. Accordingly, the final rule clarifies, in § __.4(f), that only one notice is required to be sent in connection with a joint account. A financial institution may, in its discretion, provide notices to each party to the account. This situation might arise, for instance, when a financial institution does not want one opt out election to apply automatically to all joint accountholders (see discussion of how to provide opt out notices, below).

Mergers. A few commenters requested guidance on what notices are required in the event of a merger of two financial institutions or an acquisition of one financial institution by another. In such a situation, the need to provide new initial (and opt out) notices to the customers of the entity that ceases to exist will depend on whether the notices previously given to those customers accurately reflect the

policies and practices of the surviving entity. If they do, the surviving entity will not be required under the rule to provide new notices.

As was stated in the preamble to the proposed rule, 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 policies and practices.

§ __.5 Annual privacy notice to customers required.

Section 503 of the GLB Act requires a financial institution to provide notices of its privacy policies and practices at least annually to its customers "during the continuation" of a customer relationship. The proposed rules implemented this requirement by requiring a clear and conspicuous notice that accurately reflects the privacy policies and practices then in effect to be provided at least once during any period of twelve consecutive months. The proposed rules noted that rules governing how to provide an initial notice also would apply to annual notices, and stated that a financial institution would not be required to provide annual notices to a customer with whom it no longer has a continuing relationship.

Several commenters requested that the final rule permit annual notices to be given each calendar year, instead of every twelve months. A variation suggested by a few commenters was to state that notices must be provided during each calendar year, with no more than 15 months elapsing between mailings. To clarify the extent of financial institutions' flexibility, the final rule retains the general rule requiring annual notices but then provides an example, in § __.5(a)(2)(ii), stating that a financial institution may select a calendar year as the 12-month period within which notices will be provided and provide the first annual notice at any point in the calendar year following the year in which the customer

relationship was established. The final rule also requires that a financial institution apply the 12-month cycle to its consumers on a consistent basis.

Several commenters suggested that a financial institution be permitted to make the annual notice available upon request only, particularly if there have been no material changes to the notice since it was last delivered. These commenters maintained that little value is added by providing customers with additional copies each year of the same information. Some suggested that financial institutions be permitted to provide a "short-form" annual notice, in which the institution informs its customers that there has been no change to its privacy policies and practices and that the customers may obtain a copy upon request.

The Agencies have not amended the final rule to permit this approach, for two reasons. First, the Agencies view the statute as contemplating complete disclosures annually to all customers during the duration of the customer relationship. Section 503 of the GLB Act states that “not less than annually during the continuation of [a customer] relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer [i.e., one with whom a customer relationship has been formed], ... of such financial institution’s policies and practices with respect to” the information enumerated in the statute. The Agencies believe that this provision contemplates a full set of disclosures to each customer once a year.

Second, the clarifications made in the final rule to the disclosure provisions make it clear that a financial institution is not required to provide a lengthy and detailed privacy notice to comply with the rule. Small institutions that do not share information with third parties beyond the statutory exceptions should be able to provide a short, streamlined notice. The rule also permits a financial institution to

provide annual notices to customers over the institution's web site if the customer conducts transactions electronically and agrees to such disclosures (see additional discussion of this flexibility, below, in § __.9). As a result, the final rule achieves much of the burden reduction sought by those requesting a short-form annual notice option.

Most of the remaining comments received in response to proposed § __.5 addressed the rules governing when a customer relationship is terminated. Several focused on whether "dormancy" of a deposit account, which was presented as an example in the proposed rule of when a customer relationship is terminated, should be determined according to state law or a financial institution's internal policies. These commenters were unanimous in their view that "dormancy" should be determined according to an institution's own policies, without reliance on state laws that may produce conflicting results and unnecessary burden for institutions operating in more than one state. A few commenters suggested that the final rule use "inactive" instead of "dormant" in order to avoid unintended consequences of classifying an account as dormant. In light of these comments, the final rule retains in the examples of when a customer relationship will be terminated the situation where there is no activity in a deposit account according to a financial institution's policies. The Agencies also have used the term "inactive" rather than "dormant" in § __.5(b)(2)(i) to avoid the unintended consequences posited by the comments.

A few commenters stated that the example of no communication with a customer for twelve months should be amended to clarify that promotional materials would not be considered a communication about the relationship sufficient to extend the duration of the customer relationship. These commenters generally suggested that the rule be tied to communications initiated by the

customer. The Agencies agree that a communication that merely informs a person about, or seeks to encourage use of, a financial institution's products or services is not the type of communication that signifies an ongoing relationship. The final rule has been amended in § __.5(b)(2)(iv) to reflect that the distribution of promotional materials will not prolong a customer relationship under the rule. The Agencies disagree, however, that the test should focus on whether there has been any customer-initiated contact, because there will be instances in which the customer will not initiate a contact with a financial institution within the relevant time period but nonetheless has an ongoing relationship.

§ __.6 Information to be included in initial and annual privacy notices.

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

The proposed rule implemented section 503 by requiring a financial institution to provide information concerning:

- the categories of nonpublic personal information that a financial institution may collect;
- the categories of nonpublic personal information that a financial institution may disclose;
- the categories of affiliates and nonaffiliated third parties to whom a financial institution discloses nonpublic personal information, other than those to whom information is disclosed pursuant to an exception in section 502(e) of the GLB Act;

- the financial institution's policies with respect to sharing information about former customers;
- the categories of information that are disclosed pursuant to agreements with third party service providers and joint marketers and the categories of third parties providing the services;
- a consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties;
- any disclosures regarding affiliate information sharing opt outs a financial institution is providing under the FCRA; and
- the bank's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.

The Agencies received a large number of comments concerning these requirements, with the majority of comments making the points summarized below.

Level of detail required. Many commenters offered the general observation that the level of detail that would be required under the proposed rule would result in lengthy, complicated, and ultimately confusing disclosures. These comments have led the Agencies to conclude that additional clarification is required concerning the level of detail that the Agencies expect a financial institution's initial and annual disclosures to contain.

The Agencies do not believe that the statute requires--nor do the Agencies intend to require--a financial institution to publish lengthy disclosures that identify with precision every type of information collected or disclosed, the name of every entity with whom the financial institution shares information, and a complete description of the technical specifications of how the institution protects its customers' records or the identity of each employee who has access to such records. Instead, the Agencies have

concluded that the statute, by focusing on "categories" of information and recipients of information, is intended to require notices that provide consumers with a general description of the third parties to whom a financial institution discloses nonpublic personal information, the types of information it discloses, and the other information about the institution's privacy policies and practices listed above. The final rule, like the proposal, permits a financial institution to comply with these notice requirements by providing a description that is representative of its privacy policies and practices. The Agencies believe that in most cases the initial and annual disclosure requirements can be satisfied by disclosures contained in a tri-fold brochure.

To address commenters' concerns about the likelihood that consumers will not read long, detailed disclosures, the Agencies have revised the examples of the disclosures set out in proposed § __.6(c) to clarify the level of detail that the Agencies think is appropriate under the statute. Sample clauses have been provided in Appendix A to the rules, and guidance for certain institutions has been set out later in this preamble. Because the examples are not exclusive, the final rule permits a financial institution to use different categories than those provided in the examples, thereby providing additional flexibility for financial institutions in complying with the disclosure requirements. In addition, the language in § __.6(a) that precedes the items of information to be addressed in the initial notice has been amended to clarify that a financial institution is required only to address those items that apply to the institution. Thus, for instance, if a financial institution does not disclose nonpublic personal information to third parties, it may simply omit any reference to the categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information.

As was noted in the preamble to the proposed rule, 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.

Short-form initial notice. The Agencies have reconsidered the need to give consumers a copy of a financial institution's complete initial notice when there is no customer relationship. In these circumstances, the Agencies believe that the objectives of the statute can be accomplished in a less burdensome way than was proposed. Accordingly, the Agencies have exercised their exemptive authority as provided in section 504(b) to create an exception to the general rule that otherwise requires a financial institution to provide both the initial and opt out notices to a consumer before disclosing nonpublic personal information about that consumer to nonaffiliated third parties.

This exception is set out in § __.6(d) of the final rule, which states that a financial institution may provide a "short-form" initial privacy policy notice along with the opt out notice to a consumer with whom the institution does not have a customer relationship. The short-form notice must clearly and conspicuously state that the disclosure containing information about the institution's privacy policies and practices is available upon request and provide one or more reasonable means by which the consumer may obtain a copy of the notice. This approach reflects the Agencies' belief that consumers who do not become customers of a financial institution generally will have less interest in the privacy policies of that financial institution and will benefit from obtaining a concise, but meaningful, opt out notice that informs the consumer about the categories of their information the institution intends to disclose and the categories of nonaffiliated third parties that will receive the information. Consumers who are interested in the more complete privacy disclosures will be provided with a convenient means to obtain them.

Information about affiliate sharing. Another point made by several commenters in response to proposed § __.6 was that the rule should not include a requirement that categories of affiliates with whom a financial institution shares information be included in the initial and annual notices. These commenters pointed out that the statute specifically requires disclosures of categories of nonaffiliated third parties only, and that the only statutorily mandated disclosures concerning affiliate sharing are disclosures required, if any, concerning affiliate sharing pursuant to section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (FCRA) (15 U.S.C. 1681a(d)(2)(A)(iii)).[8] These commenters concluded that the Agencies, by expanding the disclosure requirements in the manner prescribed in the proposed rule, would be exceeding their rulemaking authority and imposing unnecessary burden on financial institutions.

The Agencies believe that the language and legislative history of section 503 support requiring disclosures of affiliate sharing beyond what may be required by the FCRA. First, section 503(b) does not state that the items listed therein are to be the only items set out in a financial institution's initial and annual disclosures. Instead, it uses the nonrestrictive phrase "shall include" when discussing the contents of the disclosures, thereby preserving flexibility for the Agencies (which were expressly granted authority under section 503(a) to prescribe rules governing these notices) to require that

---

[8] 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 the disclosure of that information. The information that can be disclosed to affiliates under this provision includes, for instance, information from consumer reports and applications for financial products or services. In general, this information represents personal information provided directly by the consumer to the institution, such as income and assets, in addition to information contained within consumer reports.

additional items be addressed in the disclosures consistent with those specifically enumerated.

Second, section 503(a) states that the financial institution shall provide in its initial and annual notices "a clear and conspicuous disclosure ... of such financial institution's policies and practices with respect to--(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 502, including the categories of information that may be disclosed; ...." While the FCRA disclosures would be a subset of the disclosures required by section 503(a)(1), they may not be sufficient to fully satisfy that requirement.

Third, the legislative history of the GLB Act suggests that Congress intended for the disclosures to provide more information about affiliate sharing than what may be required under the FCRA.[9] That history underscores the Congressional intent of ensuring that individuals are given the opportunity to make informed decisions about the privacy policies and practices of financial institutions. The Agencies believe that limiting the disclosures about affiliate sharing just to those disclosures that may be required under the FCRA would frustrate that purpose.

Disclosures of the FCRA opt out right. Another commonly advanced argument was that a financial institution should not be required to include FCRA disclosures in its annual notices. As previously discussed, section 503(b)(4) of the GLB Act requires a financial institution's initial and

---

[9] See, e.g., remarks of Sen. Gramm (noting that the privacy bill contains "for the first time a full disclosure requirement. It requires every bank in America, when you open your account to tell you precisely what their policy is: Do they share personal financial information within the bank? Do they share it outside the bank?"), 145 Cong. Rec. S13786 (daily ed. Nov. 3, 1999); remarks of Sen. Hagel, id. at S13876 ("Financial institutions would be required to disclose their privacy policies to their customers on a timely basis. If customers do not believe adequate protections exist at their institution, they can take their business elsewhere.").

annual notice to include the disclosures required, if any, under section 603(d)(2)(A)(iii) of the FCRA. The proposed rules implemented section 503(b)(4) of the GLB 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. Several commenters pointed out that the FCRA requires disclosures of a consumer's right to opt out of affiliate sharing only once. They noted that the GLB Act states, in section 506(c), that nothing in the GLB Act is to be construed to modify, limit, or supersede the operation of the FCRA. These commenters maintain that the "if any" language of section 503(b)(4), read in the context of section 506, suggests that, since at most only one notice must be provided under the FCRA, section 503 should require only one FCRA disclosure under the privacy rule. The commenters concluded that, by requiring more notices than are required under the FCRA, the Agencies would be violating this express preservation of the FCRA.

As discussed above, the Agencies believe that a financial institution, in order to comply with the requirement that it disclose its policies and practices with respect to sharing information with affiliated and nonaffiliated third parties, must describe the circumstances under which it will be sharing information with affiliates. Clearly, the ability of consumers to opt out of affiliate information sharing under the FCRA affects a financial institution's policies and practices with respect to disclosing information to its affiliates. Failing to include this information and an explanation of how the opt out right may be exercised would, in the view of the Agencies, make the disclosures incomplete. Thus, a financial institution will need to include this information in its initial and annual notices.

The Agencies note, moreover, that they disagree with the commenters' reading of sections 503 and 506. Section 503 does not distinguish between the disclosures to be provided in the initial notice

from those to be provided in the annual notice. Thus, a plain reading of section 503 suggests that any disclosures that are required under the FCRA must be included in both the initial and annual notices.

The Agencies interpret the "if any" language as a recognition that not all institutions provide FCRA notices because not all institutions engage in the type of affiliate sharing covered by the FCRA. By requiring the FCRA notice to appear as part of the annual notice under the privacy rule, the Agencies believe that they are not modifying, limiting, or superseding the operation of the FCRA; financial institutions will have exactly the same FCRA obligations following the effective date of the privacy rule as they had before. The only difference will be that, as is required by the GLB Act, a financial institution's initial and annual disclosures about its privacy policy and practices will need to reflect how the financial institution complies with the affiliate sharing provisions of the FCRA.

Disclosures of the right to opt out. Other commenters suggested that the final rule eliminate the requirement that the initial and annual notices contain disclosures about a consumer's right to opt out. These commenters pointed out that the statute does not specifically require these disclosures.

As previously discussed, section 503(a) of the statute requires a financial institution to disclose its policies and practices with respect to sharing information, both with affiliated and nonaffiliated third parties. Given that a financial institution's practices with respect to sharing nonpublic personal information with nonaffiliated third parties will be affected by the opt out rights created by the statute, an institution will need to describe these opt out rights in order to provide a complete disclosure that satisfies the statute.

Other comments. The Agencies received many comments expressing support for a number of the provisions in proposed § __.6. For instance, several commenters noted their agreement with the

approach of permitting a financial institution to state generally that it makes disclosures to nonaffiliated third parties "as permitted by law" to describe disclosures made pursuant to one of the exceptions. Others agreed with the proposed flexibility to allow a disclosure to be based on current and contemplated information sharing. In light of these comments, the Agencies have adopted proposed § __.6 with changes as discussed above. The final rule makes several other stylistic changes to the material in § __.6 that are intended to make the rule easier to read.[10]

§ __.7 Form of opt out notice to consumers; opt out methods.

Paragraph (a) of proposed § __.8 required that any opt out notice provided by a financial institution be clear and conspicuous and accurately explain the right to opt out. The proposed rule also required a financial institution to provide the consumer with a reasonable means by which to opt out, required a financial institution to honor an opt out election as soon as reasonably practicable, and stated that an opt out election survived until revoked by the consumer. The Agencies received a large number of comments in response to each of these provisions, addressing the application of these rules to joint accounts, the means by which an opt out right may be exercised, duration of an opt out, the level of detail required in the opt out notice, and the time by which an opt out election must be honored. These points are addressed below.

Joint accounts. Most of the commenters on this issue stated that a financial institution should have the option of providing one notice per account, regardless of the number of persons on the account. The Agencies agree that this is appropriate, and have added a new § __.7(d) to address this

---

[10] The Agencies expect to publish proposed standards in the near future relating to administrative, technical, and physical safeguards as required by section 501(b) of the GLB Act.

issue. Under the final rule, a financial institution has the option of providing only one initial, annual, and opt out notice per account. However, any of the accountholders must have the right to opt out. The final rule requires a financial institution to state in the opt out notice provided to a joint accountholder whether the institution will consider an opt out by a joint accountholder as an opt out by all of the associated accountholders or whether each accountholder is permitted to opt out separately.

Means of opting out. Another issue addressed by many commenters concerned the means by which consumers may opt out. Several suggested that a financial institution, after having provided reasonable means of opting out, should be able to require consumers to use those means exclusively. The Agencies agree with this suggestion, recognizing that a financial institution may not have trained personnel or systems in place to handle opt out elections at each point of contact between a consumer and financial institution. Assuming a financial institution offers one or more of the opt out means provided in the examples in the final rule or a means of opting out that is comparably convenient for a consumer, the institution may require consumers to opt out in accordance with those means and choose not to honor opt out elections communicated to the institution through alternative means. A new paragraph (iv) has been added to § __.7(a)(2)(iv) to reflect this.

The final rule adds an example of a toll-free telephone number in § __.7(a)(2)(ii)(D) as another way by which financial institutions may allow consumers to opt out. As stated in § __.7(a)(2)(iii)(A), a financial institution may not require a consumer to write his or her own letter in order to opt out.

Duration of opt out. Several commenters requested that the rule concerning duration of an opt out, as provided in § __.8(e) of the proposal, be changed to require a more workable approach. These commenters noted that, under the proposal, a financial institution would be required to keep

track of opt out elections forever. To illustrate their point, the commenters posited the example of a person who opts out during the course of establishing a customer relationship with a financial institution, terminates that relationship, and then establishes another customer relationship several years later, perhaps under a different name or with someone on a joint account. The commenters suggested that it would be more appropriate in these circumstances to treat the opt out election made in connection with the first relationship as applying solely to that relationship.

The Agencies agree with the commenters' suggestions. Thus, under the final rule, a financial institution is to treat an opt out election made by a customer in connection with a prior customer relationship as applying solely to the nonpublic personal information that the financial institution collected during, or related to, that relationship. That opt out will continue until the customer revokes it. However, if the customer relationship terminates and a new one is established at a later point, the financial institution must then provide a new opt out notice to the customer in connection with the new relationship and any prior opt out election does not apply to the new relationship.

Level of detail required in opt out notice. A few commenters expressed concern about the level of detail they perceived the proposed rule to require in an opt out notice. These commenters interpreted the statement in proposed § __.8(a)(2) that a financial institution "provides adequate notice ... if [the institution] identifies all of the categories of nonpublic personal information that [the institution] discloses or reserves the right to disclose to nonaffiliated third parties as described in [§ __.6]" as requiring a more detailed disclosure of categories of nonpublic personal information and nonaffiliated third parties than is required in the initial and annual notices.

The Agencies did not intend this result, and specifically referred to § __.6 in the proposed opt

out provision to address precisely the concern raised by these commenters. The disclosures in the initial and annual notices of the categories of nonpublic personal information being disclosed and the categories of nonaffiliated third parties to whom the information is disclosed will suffice for purposes of the opt out notices as well. If the opt out notice is a part of the same document that contains the disclosures that must be included in the initial notice, then the financial institution is not required to restate the same information in the opt out notice. In this instance, the rule requires only that the categories of nonpublic personal information the institution intends to share and the categories of nonaffiliated third parties with whom it will share are clearly disclosed to the consumer when the opt out and privacy notices are read together.

One commenter suggested that, while a financial institution should have the option of providing an opt out notice that is sufficiently broad to cover anticipated disclosures, the financial institution also should be permitted to provide a customer who already has opted out with a new opt out notice in connection with a new financial product or service and, if the consumer does not opt out a second time, be free to disclose nonpublic personal information obtained in connection with that financial product or service to nonaffiliated third parties. The Agencies believe that a financial institution should be permitted the flexibility to provide opt out notices that are either narrowly tailored to specific types of nonpublic personal information and types of nonaffiliated third parties or that are more broadly worded to anticipate future disclosure plans. However, if a consumer opts out after receiving an opt out notice from a financial institution that is broad enough to cover the new type of information sharing desired by that institution, the failure of the consumer to opt out again does not revoke the earlier opt out election.

Time by which opt out must be honored. Under the proposal, a financial institution is

directed to comply with an opt out election "as soon as reasonably practicable." A large number of comments asked the Agencies to clarify in the final rule how long a financial institution has after receiving an opt out election to cease disclosing nonpublic personal information to nonaffiliated third parties. Suggestions for a more precise standard ranged from mandating that a financial institution stop disclosing information immediately to a mandatory cessation within several months of receiving the opt out. As was the case with other suggestions for bright-line standards in different contexts, the Agencies believe that it is appropriate to retain a more general rule in light of the wide range of practices throughout the financial institutions industry. A potential drawback of a more prescriptive rule is that an institution might use the standard as a safe harbor in all instances and thus fail to honor an opt out election as early as it is otherwise capable of doing. Another drawback is that a standard that is set in light of current industry practices and capabilities is likely to become outmoded quickly as advances in technology increase efficiency. The Agencies therefore decline to adopt a more rigid standard, and instead retain the rule as set out in § __.7(e) of the final rule.

For the reasons stated above, the Agencies adopt, in § __.7, the rule governing the form of opt out notices and methods of opting out as discussed above. This section contains other stylistic changes to what was proposed in order to make the final rule easier to read.

§ __.8 Revised privacy notices.

The proposed rule, in § __.8(c), prohibited a financial institution, directly or through its affiliates, from disclosing nonpublic personal information about its consumers to nonaffiliated third parties unless the institution first provided a copy of its privacy notice and opt out notice. The proposal also required that these notices be accurate when given. Thus, if an institution wants to disclose nonpublic personal

information in a way that is not accurately described in its notices, the institution would be required under the proposed rule to provide new notices before making the disclosure in question.

The Agencies received no comments raising questions about these requirements. Accordingly, the final rule adopts them, but sets them out in a separate section (§ __.8) in the final rule for emphasis. The final rule sets out examples in § __.8(b) of when a new notice would, and would not, be required.

§ __.9 Delivering privacy and opt out notices.

The proposed rules governing delivery of initial, annual, and opt out notices were set out in proposed §§ __.4(d), __.5(b), and __.8(b), respectively. Given the substantial similarities between the three sets of rules, the Agencies have decided to combine the rules in one section in order to make it easier for the reader. Accordingly, the final rule states these rules in § __.9.

The general rule requires that notices be provided in a manner so that each consumer can reasonably be expected to receive actual notice in writing, or, if the consumer agrees, electronically. The Agencies received a number of comments on the various provisions governing delivery, as discussed below.

Posting initial notices on a web site. A few commenters suggested that a financial institution be allowed to deliver initial notices simply by posting its notice on the institution's web site. The Agencies recognize that there will be instances when a notice on a web site may be delivered in a way that will enable the financial institution to reasonably expect that the consumer will receive it. The final rule retains, as an example of one way to comply with the rule, the posting of a notice on a web site and requiring a consumer to acknowledge receipt of the notice as a step in the process of obtaining a financial product or service. See § __.9(b)(1)(iii). However, the Agencies believe that the mere

posting of a notice on a web site would not be sufficient in all cases for the financial institution to reasonably expect its consumers to receive the notice. Accordingly, the Agencies have declined to expand the rule beyond the circumstance described in the example provided.

Posting annual notices on a web site. Several commenters requested that a privacy notice posted by a financial institution on its web site be deemed to satisfy the annual notice requirement, at least for customers who agree to receive notices on the institution's web site. The Agencies believe that it is appropriate to provide annual notices in this way for customers who conduct transactions electronically and agree to accept notices on a web site. Accordingly, the Agencies have amended the rule by adding a new § __.9(c)(i) to clarify that a financial institution may reasonably expect a customer who uses the institution's web site to access financial products or services will receive actual notice if the customer has agreed to accept notices at the institution's web site and the financial institution posts a current notice of its privacy policies and practices continuously and in a clear and conspicuous manner on the web site. The Agencies believe that this will reduce burden on financial institutions while ensuring that customers who transact business electronically will have continuous access to institutions' privacy policies and practices.

Disclosures to customers requesting no communication. Several commenters suggested the Agencies clarify in the final rule how the disclosure obligations may be met in the case of a customer who requests that the institution refrain from sending information about the customer's relationship. These commenters stated that, in this case, the customer's request should be honored.

The Agencies agree. When a customer provides explicit instructions for a financial institution not to communicate with that customer, the Agencies believe that the request should be honored. The

final rule clarifies, in § __.9(c)(ii), that financial institutions need not send notices to a customer who requests no communication, provided that a notice is available upon request.

Reaccessing a notice. A few commenters stated that the requirement that a privacy policy be provided in a way that enables a customer to either retain or reaccess the notice should clarify that the rule obligates a financial institution to make available only the privacy policy currently in effect. These commenters were concerned about the potential for confusion and the burden stemming from a rule that would require a financial institution to make available every version of its privacy policies. The Agencies agree that it is appropriate to require only that the current privacy policy be made available to someone seeking to obtain it after having received the initial notice, and have amended the rule accordingly in § __.9(e)(2)(iii).

Joint notices. Other commenters requested that the rule clarify that the privacy policies and practices of several different affiliated financial institutions may be described on a single notice. Related to this point, commenters requested that the final rule address whether affiliated financial institutions, each of whom has a customer relationship with the same consumer, may elect to send only one notice to the consumer on behalf of all of the affiliates covered by the notice and have that one notice satisfy the disclosure obligations under § __.4 of each affiliate. The Agencies believe that financial institutions should be able to combine initial disclosures in one document. The Agencies also believe that it is appropriate to permit financial institutions that prepare a combined initial or annual notice to give, on a collective basis, a consumer only one copy of the notice. The final rule reflects this flexibility, in § __.9(f). The Agencies emphasize that the notice must be accurate for all financial institutions using the notice and must identify by name each of the institutions. The Agencies also note that financial

institutions that provide one combined notice must be capable of keeping track of whether a consumer has opted out in order to ensure that disclosures are made in accordance with whatever opt out instructions a consumer provides after having received the joint notice.

§ __.10 Limits on disclosure of nonpublic personal information to nonaffiliated third parties.

Section 502(a) of the GLB Act generally prohibits a financial institution, directly or through its affiliates, from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution 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 implemented these provisions by requiring a financial institution to give the consumer the initial notice required by § __.4, the opt out notice required by § __.8, and a reasonable opportunity to opt out.

Most of the comments on this section focused on the question of what is a reasonable opportunity to opt out. Suggestions ranged from a financial institution having the right to begin sharing information immediately (when the opt out and initial notices are provided as part of a transaction being conducted electronically, such as might be the case in an ATM transaction) up to a mandatory delay of 120 days from the time the notices are provided.

The Agencies believe that the wide variety of suggestions underscores the appropriateness of a more general test that avoids setting a mandatory waiting period applicable in all cases. For isolated transactions where a financial institution intends to disclose nonpublic personal information that it obtains

through an electronic transaction and the consumer is provided a convenient means of opting out as part of the transaction, it would be reasonable not to force the financial institution to wait a set period of time before sharing the information. An example of this is provided at § __.10(a)(3)(iii). For other opt out notices that are provided by mail, the Agencies believe it is appropriate to allow the consumer additional time. In these latter instances, the Agencies consider it reasonable to permit the consumer to opt out by mailing back a form, by calling a toll-free number, or by any other reasonable means within 30 days from the date the opt out notice was mailed. See § __.10(a)(3)(i). The final rule also provides an example of a reasonable opportunity for opting out in connection with accounts opened on-line. See § __.10(a)(3)(ii). However, rather than try to anticipate every scenario and establish a time frame that would accommodate each, the Agencies think it is appropriate simply to state that the consumer must be given a reasonable opportunity to opt out and then provide a few illustrative examples of what would be reasonable in different contexts.

Other comments pointed out that proposed § __.7(a)(3)(i) (§ __.10(a)(3)(i) of the final rule) inappropriately implied that the opportunity to opt out by mail is available only when a consumer has a customer relationship with the financial institution. The final rule deletes the reference to a customer relationship in that section to avoid creating that implication.

§ __.11 Limits on redisclosure and reuse of information.

Section 502(c) of the GLB 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 both the financial institution and the third party, unless the disclosure would be lawful if made directly by the financial institution. The proposed

rule implemented section 502(c) by imposing limits on redisclosure that apply both to a financial institution that receives information from a nonaffiliated financial institution and to any nonaffiliated third party that receives nonpublic personal information from a financial institution. The proposed rule also imposed limits on the ability of financial institutions and nonaffiliated third parties to reuse nonpublic personal information they receive. As noted in the preamble to the proposed rule, sections 502(b)(2) and 502(e) permit disclosures of nonpublic personal information for specific purposes. The Agencies sought comment on whether the final rule should limit the ability of an entity that receives nonpublic personal information pursuant to an exception to use that information only for the purpose of that exception. The Agencies also sought comment on what the term "lawful" means in the context of section 502(c), and whether a recipient of nonpublic personal information could "lawfully" disclose information if the disclosure complied with a notice provided by the institution that made the disclosure initially. Finally, the Agencies invited comment on whether the rules should require a financial institution that discloses nonpublic personal information to a nonaffiliated third party to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of that information.

The Agencies received a large number of comments in response to this proposed section. A few opined that the Agencies would exceed their rulemaking authority if the final rule were to retain the limits on reuse of information, given that section 502(c) expressly addresses only redisclosures and not reuse. Most comments concerning proposed § __.12 stated that financial institutions should not have to monitor compliance with the redisclosure and reuse provisions of the rule, although these commenters said that financial institutions typically will contractually limit the recipient's ability to reuse information for purposes other than those for which the information was disclosed. These issues are addressed

below.

Limits on reuse. The position advanced by those critical of imposing limits on reuse is premised on the conclusion that Congress, by addressing limits on redisclosures in section 502(c), provided the only limits that may be imposed on what a recipient of nonpublic personal information can do with that information. The Agencies disagree with this premise. Section 502(c) is silent on the question of reuse, making it necessary to look to the overall purposes of the statute to determine whether the Agencies should impose limits on the ability of nonaffiliated third parties to reuse nonpublic personal information that they receive from a financial institution. The Agencies believe that the overall purposes of subpart A of Title V of the Act make it appropriate to impose limits on reuse, depending on whether the information was obtained pursuant to one of the exceptions in section 502(e) of the GLB Act (as implemented by §§ __.14 and __.15 of the final rule).

When disclosures are made in connection with one of the purposes set out in section 502(e), those disclosures are exempt from the notice and opt out protections altogether. A customer has no right to prohibit those disclosures or even to know more than that the disclosures are being made "as permitted by law." A consumer who does not establish a customer relationship is not even put on notice that the disclosures are made as permitted by law, because that consumer will not be entitled to any privacy or opt out notice. The only protection afforded by the statute for disclosures made under section 502(e) is the limited nature of the exceptions. The Agencies believe it would be inappropriate to undermine that protection by allowing the recipient of nonpublic personal information to reuse the information for any purpose, including marketing.

By contrast, when a consumer decides not to opt out after being given adequate notices and the

opportunity to do so, that consumer has made a decision to permit the sharing of his or her nonpublic personal information with the categories of entities identified in the financial institution's notices. The consumer's primary protection in the case of a disclosure falling outside the section 502(e) exceptions comes from receiving the mandatory disclosures and the right to opt out. The statute provides only the additional protection in section 502(c), restricting a recipient's ability to redisclose information to entities that are not affiliated with either the recipient or the financial institution making the disclosure initially. Thus, if a consumer permits a financial institution to disclose nonpublic personal information to the categories of nonaffiliated third parties that are described in the institution's notices, recipients of that nonpublic personal information appear authorized under the statute to make disclosures that comply with those notices.

To implement this statutory scheme, the Agencies have retained a limit on reuse in addition to the limit on redisclosures. The limits on redisclosure and reuse that apply to recipients of information and their affiliates will vary, depending on whether the information was provided pursuant to one of the 502(e) exceptions.

For nonpublic personal information provided pursuant to section 502(e), a financial institution receiving the information may disclose the information to its affiliates or to affiliates of the financial institution from which the information was received. It may also disclose and use the information pursuant to an exception in §§ __.14 or __.15 in the ordinary course of business to carry out the activity covered by the exception under which the institution received the information. The financial institution's affiliates may disclose and use the information, but only to the extent permissible for the financial institution.

For nonpublic personal information provided outside one of the section 502(e) exceptions, the financial institution receiving the information may disclose the information to its affiliates or to the affiliates of the financial institution that made the initial disclosure. It may also disclose the information to any other person, if the disclosure would be lawful if made directly by the financial institution from which the information was received. This would enable the receiving institution to disclose pursuant to one of the section 502(e) exceptions. It also would permit the receiving institution to redisclose information in accordance with the opt out and privacy notices given by the institution making the initial disclosures, as limited by any opt out elections received by that institution. The affiliates of a financial institution that receives nonpublic personal information may disclose only to the extent that the financial institution may disclose the information.

These same general rules apply to a non-financial institution third party that receives nonpublic personal information from a financial institution. Thus, the third party receiving the information pursuant to one of the section 502(e) exceptions may disclose the information to its affiliates or to the affiliates of the financial institution that made the disclosure. The third party also may disclose and use the information pursuant to one of the section 502(e) exceptions as noted in the rule. The affiliates of the third party may disclose and use the information only to the extent permissible for the third party. If the third party receives the information from a financial institution outside one of the section 502(e) exceptions, the third party may disclose to its affiliates or to the affiliates of the financial institution. It may also disclose to any other person if the disclosure would be lawful if made by the financial institution. The third party's affiliates may disclose and use the information to the same extent permissible for the third party.

In cases where an entity receives information outside of one of the section 502(e) exceptions, that entity will in essence "step into the shoes" of the financial institution that made the initial disclosures. Thus, if the financial institution made the initial disclosures after representing to its consumers that it had carefully screened the entities to whom it intended to disclose the information, the receiving entity must comply with those representations. Otherwise, the subsequent disclosure by the receiving entity would not be in accordance with the notices given to consumers and would not, therefore, be lawful. Even if such representations do not prevent the recipient from redisclosing the information, the recipient's ability to redisclose will be limited by whatever opt out instructions were given to the institution making the initial disclosures and by whatever new opt out instructions that are given after the initial disclosure. The receiving entity, therefore, must have procedures in place to continually monitor the status of who has opts out and to what extent. Given these practical limitations on the ability of a recipient to disclose pursuant to another institution's privacy and opt out notices, redisclosure of information is most likely to arise under one of the section 502(e) exceptions (as implemented by §§ __.14 and __.15 of the final rule).

Monitoring third parties. The Agencies have decided not to amend their respective rules to impose a specific duty on financial institutions to monitor third parties' use of nonpublic personal information provided by the institutions. This does not address whether obligations to do so may arise in other contexts. The Agencies note, for instance, that most of the commenters who requested that the Agencies not impose such a duty stated that they have contracts in place that limit what the recipient may do with the information. The Agencies also note that the limits on reuse as stated in the final rule provide a basis for an action to be brought against an entity that violates those limits.

§ __.12 Limits on sharing account number information for marketing purposes.

Section 502(d) of the GLB Act prohibits a financial institution from disclosing, "other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer." Proposed § __.13 applied this statutory prohibition to disclosures made directly or indirectly by a financial institution, and sought comment on whether one or more exceptions to the flat prohibition should be created.

The Agencies received comments from people who suggested that various exceptions be created as well as from people who believe that a flat prohibition is necessary to protect consumers from unscrupulous practices. After considering the suggestions from all of the commenters addressing this issue, the Agencies have decided to amend proposed § __.13 by (a) adding two exceptions that the Agencies believe are necessary for financial institutions to engage in legitimate, routine business practices and that are unlikely to pose a significant potential for abuse and (b) clarifying that the prohibition does not apply in two circumstances frequently mentioned in the comments. These exceptions and clarifications are discussed below.

Disclosures to a financial institution's agent or service provider. Many financial institutions noted that they use agents or service providers to conduct marketing on the institution's behalf. This might occur, for instance, when an insured depository institution instructs a service provider that assists in the delivery of monthly statements to include a "statement stuffer" with the statement informing consumers about a financial product or service offered by the institution. The

Agencies recognize the need to disclose account numbers in this instance, and believe that there is little risk to the consumer presented by such disclosure.

Similarly, the Agencies recognize that a financial institution may use agents to market the institution's own financial products and services. Commenters advocating that the final rule exclude disclosures to agents stated that the agents effectively act as the financial institution in the marketing of the institution's financial products and services. These commenters suggested that there was no more reason to preclude sharing the account numbers with an agent hired to market the institution's financial products and services than there would be to preclude sharing between two departments of the same institution. The Agencies are concerned, however, about the possibility of transactions being consummated by a financial institution's agent who may be engaging in practices contrary to the institution's instructions. While the Agencies recognize that a financial institution frequently will use agents to assist it in marketing its products, the Agencies believe that a consumer's protections are potentially eroded by allowing agents to have access to a consumer's account. Accordingly, the Agencies have added an exception in § __.12(b)(1) that would permit disclosures of account numbers by a financial institution to an agent for the purpose of marketing the financial institution's financial product or services, but have qualified that exception by stating that the agent has no authority to initiate charges to the account.

Private label credit cards and affinity programs. Many commenters stated that the final rule should not prevent the disclosure of account numbers in the situation where a consumer chooses to participate in a private label credit card program or other affinity program. Under these programs, a consumer typically will be offered certain benefits, often by a retail merchant, in return for using a credit

card that is issued by a particular financial institution. The commenters suggested that, in the example of an affinity program, the consumer understands the need for the merchant and financial institution to share the consumer's account number. The Agencies agree that this type of disclosure is appropriate and does not create a significant risk to the consumer. Accordingly, § __.12(b)(2) has been added to the final rule to exclude the sharing of account numbers where the participants are identified to the consumer at the time the consumer enters into the program.

Encrypted numbers. Many commenters urged the Agencies to exercise their exemptive authority to permit the transmission of account numbers in encrypted form. Several commenters noted that encrypted account numbers and other internal identifiers of an account are frequently used to ensure that a consumer's instructions are properly executed, and that the inability to continue using these internal identifiers would increase the likelihood of errors in processing a consumer's instructions. These commenters also point out that if internal identifiers may not be used, a consumer would need to provide an account number in order to ensure proper handling of a request, which would expose the consumer to a greater risk than would the use of an internal tracking system that preserves the confidentiality of a number that may be used to access the account.

The Agencies believe an encrypted account number without the key is something different from the number itself and thus falls outside the prohibition in section 502(d). In essence, it operates as an identifier attached to an account for internal tracking purposes only. The statute, by contrast, focuses on numbers that provide <u>access</u> to an account. Without the key to decrypt an account number, an encrypted number does not permit someone to access an account.

In light of the statutory focus on access numbers, and given the demonstrated need to be able to

identify which account a financial institution should debit or credit in connection with a transaction, the Agencies have included a clarification in § __.12(c)(1) of the final rule stating that an account number, or similar form of access number or access code, does not include a number or code in an encrypted number form, as long as the financial institution does not provide the recipient with the means to decrypt the number. The Agencies believe that consumers will be adequately protected by disclosures of encrypted account numbers that do not enable the recipient to access the consumer's account.

Definition of "transaction account." Several commenters suggested that the final rule clarify that accounts to which no charge may be posted are not covered by the prohibition against disclosing account numbers. These commenters frequently cited mortgage loan accounts as typical of those that should fall outside the scope of the prohibition. The Agencies agree with the principle behind these suggestions. However, the Agencies note that there have been instances in which a borrower's monthly payments on a mortgage loan have been increased in connection with the marketing of a financial product or service without the borrower's knowledge or permission. Accordingly, the final rule clarifies, in § __.12(c)(2), that a transaction account is an account other than a deposit account or a credit card account, and does not include an account to which third parties cannot initiate charges. If it would be possible, for instance, for a third party marketer to initiate a charge to a mortgage loan account, then the final rule would prohibit the disclosure of that account number to the marketer.

§ __.13 Exception to opt out requirements for service providers and joint marketing.

Section 502(b) of the GLB 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 "fully discloses" to the consumer that it will provide this information to the nonaffiliated third party before the information is shared and enters into a contract with the third party that requires the third party to maintain the confidentiality of the information. As noted in the proposed rule, this contract should be designed to ensure that the third party (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 majority of the comments on this exception expressed concern that routine servicing agreements between a financial institution and, for instance, a loan servicer would be subject to the requirements of proposed § __.9 (§ __.13 in the final rule). These commenters consistently pointed out that section 502(e) of the GLB Act contains several exceptions for the sharing of information by a financial institution that is necessary to permit a third party to perform services for a financial institution. The commenters requested clarification that disclosures made pursuant to one of the section 502(e) exceptions are not subject to the requirements imposed on disclosures made pursuant to section 502(b)(2) of the GLB Act. The Agencies agree that when a disclosure may be made under section 502(e), the statute permits that disclosure without the financial institution first complying with the requirements imposed by section 502(b)(2).

A related issue is whether a financial institution must satisfy the disclosure obligations of section

502(b)(2) and have a confidentiality agreement in the case of a service provider that is performing an activity governed by section 502(b)(2) (i.e., those that are not covered by one of the section 502(e) exceptions). Several commenters maintained that it is illogical to impose a set of requirements on disclosures to the section 502(b)(2) service providers when no such requirements are imposed on the section 502(e) service providers. The Agencies believe, however, that a plain reading of section 502(b)(2) leads to that result.[11] The Agencies read the phrase "if the financial institution fully discloses..." as used in section 502(b)(2) as modifying the phrase "This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution,...." The Agencies thus have concluded that any disclosure to a service provider not covered by section 502(e) must satisfy the disclosure and written contract requirements of section 502(b)(2).

Several other commenters addressed the question of whether the rule should include safeguards beyond those provided by the statute to protect a financial institution from the risks that can arise from agreements with third parties. Most suggested that safety and soundness concerns were more appropriately addressed in a forum other than a rule designed to protect consumers' financial privacy.

---

[11] The statute states, in relevant part, that section 502(b) --

> shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including the marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

Others opined that financial institutions did not need the rule to mandate certain protections on their behalf. The Agencies have concluded that the protections set out in the statute, as implemented by § __.13(a)(1)(ii), are adequate for purposes of the privacy rule. Those protections require a financial institution to provide the initial notice required by § __.4 of the final rule as well as enter into a contractual agreement with a third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the bank disclosed the information, including use under an exception in §§ __.14 or __.15 in the ordinary course of business to carry out those purposes. These limitations will preclude recipients from sharing a consumer's nonpublic personal information pursuant to a chain of third party joint marketing agreements.

Several commenters asked whether a financial institution would have to modify existing contracts with third parties to comply with the rule. The Agencies believe that a balance must be struck that minimizes interference with existing contracts while preventing evasions of the regulation. To achieve these goals, the final rule states, in § __.18(c), that contracts in effect as of July 1, 2000 must be brought into compliance with the provisions of § __.9 by July 1, 2002.

For the reasons expressed above, the Agencies have adopted, in § __.13 of the final rule, the provisions that were set out in § __.9 of the proposal with the changes noted above. The Agencies note that financial institutions should remain vigilant in their efforts to ensure that agreements they enter into with third parties do not expose the institutions to undue risks. These risks are particularly prevalent in arrangements whereby a financial institution endorses or sponsors a financial product or service offered by the third party.

§ __.14 Exceptions to notice and opt out requirements for processing and servicing

transactions.

As previously discussed, section 502(e) of the GLB 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. Proposed § __.10 implemented those exceptions by restating them with only stylistic changes that were intended to make the exceptions easier to read. The preamble to that proposed section noted that the exceptions set out in proposed § __.10 (as well as the exceptions set out in § __.11 of the proposal) 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.

The Agencies received several comments from institutions pointing out that, by deleting the statutory phrase “in connection with” from the exceptions for information shared (a) to service or process a financial product or service requested by the consumer or (b) to maintain or service a customer account, the Agencies narrowed the application of the exception. The Agencies did not intend this result, and have changed the final rule accordingly. See § __.14(a).

Several other commenters requested that the final rule specifically state that certain services, such as those provided by attorneys, appraisers, and debt collectors (as appropriate), are “necessary” to effect, administer, or enforce a transaction, as that term is used in paragraph (a) and defined in paragraph (b) of proposed § __.10. Others cited examples of entities seeking to verify funds availability or obtain loan payoff information as instances where a disclosure would fall within the exceptions described in proposed § __.10. The Agencies believe that disclosures to these types of

professionals and under the circumstances posited by the commenters may be necessary to effect, administer, or enforce a transaction in a given situation. However, the Agencies have not listed specific types of disclosures in the regulation as necessarily falling within the scope of the exception because they are concerned that a general statement could be applied inappropriately to shelter disclosures that, in fact, are not necessary to effect, administer, or enforce a transaction.

Other commenters suggested that the final rule clarify, in situations where a financial institution uses an agent to provide services to a consumer, that the consumer need not have directly requested or authorized the service provider to provide the financial product or service but may request it from the principal instead. The Agencies agree that the communication may be between the consumer and the service provider, and note that the rule governing agents as set out in the definition of "consumer," above, provides the flexibility sought by the commenters. Briefly stated, an individual will not be a consumer of an entity that is acting as agent for another financial institution in connection with that financial institution's providing a financial product or service to the consumer.

§ __.15 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 set out those exceptions for disclosures that are not made in connection with the administration, processing, servicing, and sale of a consumer's account, and made stylistic changes to the statutory language intended to clarify the exceptions. The proposal also provided an example of the consent exception in the context of a financial institution that has received an application from a consumer for a mortgage loan informing a nonaffiliated insurance company that the consumer has

applied for a loan. The Agencies invited comment on whether safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion.

Several commenters responded to the request for comment on whether the consent exception should include safeguards, such as a requirement that the consent be written, be indicated by a signature on a separate line, or automatically terminate after a certain period of time. Of these, some favored the additional safeguards discussed in the proposal, while others maintained that safeguards are unnecessary. Several suggested that the consent exception include a provision noting that participation in a program where a consumer receives "bundled" products and services (such as would be the case, for instance, in an affinity program) necessarily implies consent to the disclosure of information between the entities that provide the bundled products or services. Others suggested that certain terms and conditions be imposed on any consent agreement, such as a time by which the financial institution must stop disclosing nonpublic personal information once a consent is revoked.

The Agencies have declined to elaborate on the requirements for obtaining consent or the consumer safeguards that should be in place when a consumer consents. The Agencies believe that the resolution of this issue is appropriately left to the particular circumstances of a given transaction. The Agencies note that any financial institution that obtains the consent of a consumer to disclose nonpublic personal information should take steps to ensure that the limits of the consent are well understood by both the financial institution and the consumer. If misunderstandings arise, consumers may have means of redress, such as in situations when a financial institution obtains consent through a deceptive or fraudulent practice. Moreover, a consumer may always revoke his or her consent. In light of the

safeguards already in place, the Agencies have decided not to add safeguards to the consent exception.

Many commenters offered specific suggestions for additional exceptions or amendments to the proposed exceptions. In many cases, the suggestions are accommodated elsewhere in the regulation (such as is the case, for instance, for exceptions to permit (a) verification of available funds or (b) disclosures to or by appraisers, flood insurers, attorneys, insurance agents, or mortgage brokers to effect a transaction). In other cases, the suggestions are inconsistent with the statute (as is the case, for instance, with one commenter's suggestion that the Agencies completely exempt a financial institution from all of the statute's requirements if the institution makes no disclosures other than what is permitted by section 502(e)). While the Agencies recognize the merits of many of the remaining suggestions, they believe that the volume and complexity of these suggestions exceed what is appropriate in a regulation. Accordingly, the Agencies have retained, in § __.15, the statement of the exceptions as proposed and invite interested parties to pursue with the Agencies clarifications as necessary in their particular circumstance.

§ __.16 Protection of Fair Credit Reporting Act.

Section 506 of the GLB Act 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 of the GLB Act is to be construed to modify, limit, or supersede the operation of the FCRA, and no inference is to be drawn on the basis of the provisions of Title V whether information is transaction or experience information under section 603 of the FCRA. Proposed § __.14 implemented section 506(c) of the GLB Act by restating the statute, making only minor stylistic changes intended to

make the rule clearer.

Comments about this provision focused on whether the Agencies, by requiring annual notice of a consumer's right to opt out under the FCRA, were modifying, limiting, or superseding the operation of the FCRA. For the reasons explained in the discussion of § __.6, above, the Agencies do not believe that the annual disclosure mandated by the GLB Act affects in any way the obligations imposed by the FCRA.

The Agencies received no other comment on this section, and, therefore, adopt the text set out in § __.14 of the proposal. See § __.16.

§ __.17 Relation to State laws.

Section 507 of the GLB 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, and may be initiated by any interested party or on the FTC's own motion. Proposed § __.15 essentially restated 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.

Comments on this section ranged from those who suggested that federal law should preempt state law in every case where there is a conflict to those who encouraged the Agencies to support the rights of states to enact greater protections. Some requested clarification of whether a particular state law would be considered more restrictive, while others suggested that the Agencies establish in the final

rule a choice of law principle for financial institutions operating in more than one state. The Agencies believe that these and other suggestions made by the commenters exceed the scope of this rulemaking and are better addressed, to the extent the Agencies have authority to address them, in other forums. Accordingly, the Agencies have adopted the text set out in proposed § __.15. See § __.17 of the final rule.

§ __.18 Effective date; transition rule.

Section 510 of the GLB 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, i.e., November 12, 2000. However, section 510(1) authorizes the Agencies to prescribe a later date in the rules enacted pursuant to section 504. The proposed rule sought comment on the effective date prescribed by the statute. It also would have required that financial institutions provide initial notices, within 30 days of the effective date of the final rule, to people who were customers as of the effective date. The preamble to the proposed rule noted that a financial institution would have to provide opt out notices before the rule's effective date if the institution wanted to continue sharing nonpublic personal information with nonaffiliated third parties without interruption.

The overwhelming majority of commenters addressing this provision requested additional time to comply with the final rule. Commenters stated that six months would not be sufficient to take the steps needed to comply with the regulation, including preparing new disclosure forms, developing software needed to track opt outs, training employees, creating management oversight systems, and undergoing internal examination and auditing to ensure compliance. Several commenters suggested that it would be less effective and potentially more confusing for consumers to receive several notices all

around the end of the year 2000 than it would be for the notices to be delivered during a rolling phase-in. Others noted that the proposed effective date would place a severe strain on financial institutions at a time when other year-end notices need to be prepared and delivered. Several commenters noted that financial institutions have not budgeted for the expenses in the current year that likely will be incurred. They also noted that the disclosures regarding the standards to be followed to protect customers' records have not been proposed for comment, thereby making it impossible for financial institutions to know how to prepare at least that part of the initial privacy notices. Requests for extensions of the effective date typically ranged from 12 months to 24 months from the date the final rules are published.

Many commenters also stated that a 30-day phase-in for initial notices to existing customers is not feasible, given the large number of notices, the short period of time allowed, and the competing demands on financial institutions at the time when the initial notices must be sent. A few suggested that the rule require initial notices to be sent only to people who establish customer relationships after the effective date of the rule, and allow a financial institution to send annual notices to existing customers at some point during the next 12 months and annually thereafter.

The Agencies agree that six months may be insufficient in certain instances for a financial institution to have ensured that its forms, systems, and procedures comply with the rule. In order to accommodate situations requiring additional time, the Agencies have retained the effective date of November 13, but, consistent with their authority under section 510(1) of the GLB Act to extend the effective date, the Agencies will give financial institutions until July 1, 2001 to be in full compliance with the regulation. Financial institutions are expected, however, to begin compliance efforts promptly, to use the period prior to June 30, 2001, to implement and test their systems, and to be in full compliance

by July 1, 2001. Given that this provides financial institutions with slightly over 13 months in which to comply with the rule, the Agencies have determined that there no longer is any need for a separate phase-in for providing initial notices. Thus, a financial institution will need to deliver all required opt out notices and initial notices before July 1, 2001.

Financial institutions are encouraged to provide disclosures as soon as practicable. Institutions that do not disclose nonpublic personal information to third parties have fewer burdens under the regulation (both in terms of the notice requirements and opt out mechanism) and should therefore be able to provide privacy notices to their consumers more expeditiously. Depending on the readiness of an institution to process opt out elections, institutions might wish to consider including the privacy and opt out notices in the same mailing as is used to provide tax information to consumers in the first quarter of 2001 to increase the likelihood that a consumer will not mistake the notices for an unwanted solicitation. The Agencies believe that this extension represents a fair balance between those seeking prompt implementation of the protections afforded by the statute and those concerned about the reliability of the systems that are put in place.

The Agencies have concluded that the extension of the date by which financial institutions must be in full compliance provides much of the relief sought by those who suggested that initial notices should not be required for existing customers. By allowing financial institutions to deliver notices over a significantly longer period of time than was proposed, the concentrated burden that would have been imposed by the proposed rule is avoided. Accordingly, the Agencies have decided not to adopt the suggestion that initial notices be required only for new customers after the effective date of the rule.

Initial notices need not be given to customers whose relationships have terminated prior to the

date by which institutions must be in compliance with the rule. Thus, if an account is inactive according to a financial institution's policies before July 1, 2001, then no initial notice would be required in connection with that account. However, because these former customers would remain consumers, a financial institution would have to provide a privacy and opt out notice to them if the financial institution intended to disclose their nonpublic personal information to nonaffiliated third parties beyond the exceptions in §§ __.14 and __.15.

The Agencies note that full compliance with the rule's restrictions on disclosures is required on July 1, 2001. To be in full compliance, institutions must have provided their existing customers with a privacy notice, an opt out notice, and a reasonable amount of time to opt out prior to that date. If these have not been provided, the disclosure restrictions will apply. This means that an institution would have to cease sharing customers' nonpublic personal information with nonaffiliated third parties on that date, unless it may share the information pursuant to an exception under §§ __.14 or __.15. Financial institutions that both provide the required notices and allow a reasonable period of time to opt out before July 1, 2001, may continue to share nonpublic personal information after that date for customers who do not opt out.

Appendix A--Sample Clauses

In order to provide additional guidance to financial institutions concerning the level of detail the Agencies believe is appropriate under the statute, the Agencies have prepared a variety of sample clauses for financial institutions to consider. The Agencies urge financial institutions to carefully review whether these clauses accurately reflect a given institution's policies and practices before using the clauses. Financial institutions are free to use different language and to include additional detail as they

think is appropriate in their notices.

Derivation chart

Below is a chart showing the derivation of the sections in the final privacy rule from the proposal. Only changes are noted.

Proposal	Content of Provision	Final Rule
4(d)	How to provide initial notice	9(a)
N/A	New product for existing customer	4(d)
4(d)(3)	Oral delivery	9(d)
4(d)(4)	Retainable notice	9(e)
N/A	Joint relationships (privacy notice)	4(f)
5(b)	How to provide annual notice	9(a)
5(b)	Actual notice of annual notice	9(c)
5(c)	Terminated customer relationships	5(b)
N/A	Delivering short-form initial notices	6(d)
7	Main operative provision	10
8(a)	Opt out methods and opt out notice content	7(a)
8(b)(1)	How to deliver opt out notices	9(a)
8(b)(2)	Oral delivery	9(d)
8(b)(3)	Same form as initial notice	7(b)
8(b)(4)	Initial notice must accompany opt out notice	7(c)
N/A	Joint relationships (opt out notice)	7(d)
8(d)	Time to comply with opt out; continuing right to opt out	7(e) & (f)
8(e)	Duration of opt out	7(g)
8(c)(1)	Revised notices	8(a)

8(c)(2)	How to deliver revised notice	8(c)
8(c)(3)	Examples of when revised notice is required	8(b)
9	Exception for service providers and joint marketers	13
10	Exceptions for processing and servicing transactions	14
11	Other exceptions	15
12	Redisclosure and reuse	11
13	Sharing account number information	12
14	FCRA	16
15	State law	17
16	Effective date	18

IV. Guidance for Certain Institutions

To minimize the burden and costs to a financial institution ("you") and generally clarify the operation of the final rule, the Agencies have included this guidance that you may use in conjunction with the sample clauses in Appendix A. This guidance specifically applies to you if you:

(1) do not have any affiliates;

(2) only disclose nonpublic personal information to nonaffiliated third parties in accordance with an exception under §§ __.14 or ___.15, such as in connection with servicing or processing a financial product or service that a consumer requests or authorizes ; and

(3) do not reserve the right to disclose nonpublic personal information to nonaffiliated third

parties, except under §§ __.14 and ___.15.[12]

In addition, if you disclose nonpublic personal information in accordance with the exception in § __.13, for service providers and joint marketers, you also must include an accurate description of that information, as illustrated by the sample clause in section (*K*) below.

In general, if you disclose nonpublic personal information to nonaffiliated third parties only as authorized under an exception, then your only responsibilities under the regulation are to provide initial and annual notices to each of your customers. You do not need to provide an opt out notice or opt out rights to your customers.

A. Initial notice to customers. You must provide an initial notice to each of your customers. A customer is a natural person who has a continuing relationship with you, as described in § __.4(c). For instance, an individual who opens a credit card or checking account with you is your customer. By contrast, an individual who uses your ATM to withdraw funds from a checking account at another financial institution is not your customer. Even if an individual repeatedly uses your ATM that individual is not your customer. In other words, you must provide initial and annual notices to each of your customers, but not to others.

B. Time to provide initial notice. You must provide an initial privacy notice to each of your customers not later than when you establish a customer relationship (§ __.4(a)(1)). For instance, you

---

[12] If you disclose or reserve the right to disclose nonpublic personal information to a nonaffiliated third party under other circumstances, you must comply with other provisions in the rule, notably §§ __.7, __.8, and __. 13, if applicable. If you disclose or reserve the right to disclose nonpublic personal information to an affiliate you must comply with other provisions in the rule, notably § __.6(a)(7), as applicable.

must provide a privacy notice to an individual not later than when that individual executes the contract to open a checking account. Thus, you can provide the notice to a checking account customer together with the account agreement and signature card.

Similarly, in the case of a loan, you must provide a privacy notice to an individual not later than when that individual executes the loan contract. For example, you can provide the notice to an individual together with the documents (or other forms) that constitute the loan contract. You may always deliver your privacy notices earlier than required.

If one of your existing customers obtains a new financial product or service from you, then you need not provide another initial notice to that customer (§ __.4(d)) if that earlier notice covered the subsequent product.

For instance, if Alison Individual walks into Bank for the first time on July 2, 2001, to open a checking account, then Bank complies with § __.4(a)(1) of the rule if it provides an initial notice to Alison together with the deposit contract. When Alison opens her checking account, she becomes a customer of Bank. Alison maintains her checking account and, six months later, returns to Bank to obtain a loan. If the initial notice that Bank provided to Alison was accurate with respect to that loan, then Bank need not provide another initial notice to her when she obtains the loan because it has provided a notice to Alison that covered the loan when she opened her checking account.

C. Method of providing the initial notice. You must provide your initial notice so that each customer can reasonably be expected to receive actual notice of it, in writing (§ __.9(a)). For example, you may provide the initial notice by mailing a printed copy of it together with a loan contract. Similarly, you may provide the initial notice by hand-delivering a printed copy of it to the customer together with a

deposit account agreement.

D. Compliance with initial notice requirement for existing customers by effective date. You must provide an initial notice to each of your current customers not later than July 1, 2001 (§ __.18(b)). You may do so by mailing a printed copy of the notice to the customer's last known address.

E. Annual notice. During the continuation of the customer relationship, you must provide an annual notice to the customer, as described in § __.5(a). You must provide an annual notice to each customer at least once in any period of 12 consecutive months during which the customer relationship exists. You may define the 12-consecutive-month period, but must consistently apply that period to the customer. You may define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice.

For example, assume that Bank defines the 12-consecutive-month period as a calendar year and provides annual notices to all of its customers on October 1 of each year. If Alison Individual opens a checking account with a Bank on July 2, 2001, thereby becoming a customer, then Bank must provide an initial notice to Alison together with the deposit agreement or earlier. Bank must provide an annual notice to Alison by December 31, 2002. If Bank provides an annual notice to Alison on October 1, 2002, as it does for other customers, then it must provide the next annual notice to Alison not later than October 1, 2003.

F. Method of providing the annual notice. Like the initial notice, you must provide the annual notice so that each customer can reasonably be expected to receive actual notice of it, in writing

(§ __.9(a)). You may do so by mailing a printed copy of the notice to the customer's last known address.

G. Joint accounts. If two or more customers jointly obtain a financial product or service, then you may provide one initial notice to those customers jointly. Similarly, you may provide one annual notice to those customers jointly (§ __.4(f)).

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

1. The categories of nonpublic personal information that you collect (§ __.6(a)(1));

2. The fact that you do not disclose nonpublic personal information about your current and former customers to affiliates or nonaffiliated third parties, except as authorized by §§ ___.14 and ___.15 (§ __.6(a)(2)-(4)). When describing the categories with respect to those parties, you are required to state only that you make disclosures to other nonaffiliated third parties as permitted by law (§ __.6(c));

3. Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (§ __.6(a)(8)).

For each of these four items of information above, you may use a sample clause from Appendix A. The Agencies emphasize that you may use a sample clause only if that clause accurately describes your actual policies and practices.

I. Example of notice. A financial institution ("Bank") that (i) does not have any affiliates and (ii) only discloses nonpublic personal information to nonaffiliated third parties as authorized under §§ ___.14 and ___.15, may comply with the requirements of § __.6 of the rule by using the following

notice, if applicable.

Bank collects nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us or others; and
- Information we receive from a consumer reporting agency. [13]

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

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

Bank restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. Bank maintains physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

J. Initial and annual notices must be clear and conspicuous. The Agencies emphasize that you must ensure that both the initial and annual notices are clear and conspicuous, as defined in § __.3(b).

K. Example of notice for disclosure to service providers and joint marketers. If you disclose nonpublic personal information in accordance with the exception in § __.13, for service providers and

[13] You need to describe only those general categories that apply to your policies and practices. Accordingly, if you do not collect information from "a consumer reporting agency," for instance, then you need not describe that category in your notices.

joint marketers, you also must include an accurate description of that information. You may comply with the requirements of § __.13 of the rule by including the following sample clause, if applicable, in the example of notice described in section *(I)* above:

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

V. Regulatory Analysis

A. Paperwork Reduction Act

The Agencies may not conduct or sponsor, and an organization is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. The OMB control numbers are listed below.

OCC:

Board:

FDIC:

OTS:

The Agencies sought comment on the burden estimates for the information collections listed below. Many commenters suggested, in response to specific proposed sections, that the rule would impose significant burden on them. Most of those suggestions concerned requirements that are imposed by the statute (such as the need to provide annual notices if an institution's previous notice remains accurate or the need to provide any notices at all in situations where an institution does not disclose nonpublic personal information to nonaffiliated third parties). The Agencies have attempted to

address other concerns by amending several provisions as discussed above and by clarifying the Agencies' expectations as far as disclosures are concerned. Below is a brief summary of the remaining paperwork burdens implemented by this final rule.

The final rule contains several disclosure requirements. The respondents must prepare and provide the initial notice to all current customers and all new customers not later than when a respondent establishes a customer relationship (§ __.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 (§ __.5(a)). The opt out notice (and partial opt out notice, if applicable; see § __.10(c)) 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 (§ __.8(a)).

The final regulation also contains affirmative actions that consumers must take to exercise their rights. In order for consumers to prevent financial institutions from sharing their information with nonaffiliated third parties, they must opt out (§§ __.7(a)(2)(ii)), __.10(a)(2) and __.10(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 (§§ __.7(f) and (g)).

OCC: The rule requires the collection of certain information from national banks, District of Columbia banks, and Federal branches and agencies of foreign banks. OMB has reviewed and approved the collections of information contained in the notice of proposed rulemaking under control number 1557-0216, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C.

3501 et seq.). OMB clearance will expire on March 31, 2003. There are 2,400 respondents with a total annual burden of 108,000 hours.

Board: The rule requires the collection of certain information from 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. In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3506; 5 CFR 1320 Appendix A.1), the Board approved the rule under the authority delegated to the Board by OMB. The OMB control number is 7100-0294. There are 9,500 respondents with a total annual burden of 427,500 hours.

FDIC: The rule requires the collection of certain information from insured nonmember banks, insured state branches of foreign banks, and certain subsidiaries of these entities. The Office of Management and Budget (OMB) has reviewed and approved the collections of information contained in the notice of proposed rulemaking under control number 3064-0136, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 et seq.). OMB clearance will expire on April 30, 2003. There are 5,764 respondents with a total annual burden of 259,380 hours.

OTS: The rule requires the collection of certain information from savings associations and certain of their subsidiaries. OMB has reviewed and approved the collections of information contained in the notice of proposed rulemaking under control number 1550-0103, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 et seq.). OMB clearance will expire on April 30, 2003. There are 1,104 respondents with a total annual burden of 49,680 hours.

The Agencies have a continuing interest in the public's opinion regarding collections of

information. Members of the public may submit comments, at any time, regarding any aspect of these collections of information. Comments may be sent to:

OCC: Communications Division, Attention: 1557-0216, Office of the Comptroller of the Currency, 250 E Street, SW, Third Floor, Washington, D.C. 20219.

Board: Mary M. West, Federal Reserve Board Clearance Officer, Mail Stop 97, Division of Research and Statistics, Board of Governors of the Federal Reserve System, Washington, D.C. 20551.

FDIC: Steven F. Hanft, Assistant Executive Secretary (Regulatory Analysis), Federal Deposit Insurance Corporation, Room F-4080, 550 17th Street NW, Washington, D.C. 20429.

OTS: Dissemination Branch (1550-0103), Office of Thrift Supervision, 1700 G Street, NW, Washington, D.C. 20552.

A copy of all comments should also be sent to Office of Management and Budget, Paperwork Reduction Project (include OMB control number), Washington, D.C. 20503.

B. Regulatory Flexibility Act

OCC: Under the Regulatory Flexibility Act (RFA), the OCC must either provide a Final Regulatory Flexibility Analysis (FRFA) with a final rule or certify that the final rule "will not, if promulgated," have a significant economic impact on a substantial number of small entities.[14] Given

[14] 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.

that the burden imposed on small institutions stems in large part from the statute, and in light of the significant number of changes described previously that reduce the rule's burden on financial institutions of all sizes, the OCC does not expect that the rule will have a significant economic impact on a substantial number of small entities. However, because the statute creates a set of requirements that are new both to the OCC and to financial institutions in general, the OCC has prepared the following FRFA and intends to publish a compliance guide for small entities.

A. Need for and Objectives of the Final Rule; Legal Basis for the Rule

The final rule implements the provisions of Title V, Subtitle A of the GLB Act addressing consumer privacy. In general, these statutory provisions require banks to provide notice to consumers about a bank's privacy policies and practices, restricts institutions from sharing nonpublic personal information about consumers to nonaffiliated third parties, and permits consumers to prevent institutions from disclosing nonpublic personal information about them to certain non-affiliated third parties by "opting out" of that disclosure.

Section 504 of the GLB Act authorizes the OCC to prescribe "such regulations as may be necessary" to carry out the purposes of Title V, Subtitle A. If no regulations were promulgated, substantive burdens imposed by the Act (e.g., the notice, information sharing restrictions, and opt out requirements) would have become effective and binding on banks one year from the date the Act was signed into law. The OCC believes that a regulatory promulgation gives the private sector greater certainty about how to comply with the statute and clearer guidance regarding how it will be enforced.

B. Small Entities to Which the Rule Will Apply

The proposed rule would apply to all banks, regardless of size, including those with assets of

under $100 million. As of December 1999, 1203 (of 2365 total) national banks had assets of under $100 million. As explained below, Title V, Subtitle A of the GLB Act did not provide a general exception for small banks, nor did it appear that such an exception would be consistent with the purposes of the Act.

C. Compliance Requirements and Effects of the Final Rule on Small Entities

A detailed description of the final rule's requirements is set forth above in the section-by-section analysis (Supplementary Information, part III). Among other things, a bank will generally be required to prepare a notice of its privacy policies and practices and provide that notice to consumers under conditions as specified in the rule (e.g., a privacy notice must be provided no later than the time that a customer relationship is established and then once annually for the duration of that customer relationship). Banks that disclose nonpublic personal information about consumers to nonaffiliated third parties will be subject to additional mandates, including a requirement to provide an opt out notice to consumers along with a reasonable opportunity to opt out of certain disclosures.

There are a host of exceptions to the general rules stated above. For example, a bank may share a consumer's nonpublic personal information with nonaffiliated third parties without having to give an opt out notice if such sharing is necessary to effect, administer, or enforce a transaction requested or authorized by the consumer. These exceptions have the effect of minimizing the burden on institutions of all sizes.

To comply with the final rule, banks will need to, among other things, prepare disclosure forms, make various operational changes, and train staff. Professional skills needed to comply with the final rule may include clerical, computer systems, personnel training, as well as legal drafting and advice.

The compliance requirements and costs are likely to vary considerably among institutions, depending upon a number of factors, such as:

--Whether a bank intends to disclose covered information. A bank that does not disclose nonpublic personal information about consumers to third parties (or shares only to the extent permitted under the exceptions) (i) could have a streamlined privacy notice, (ii) will not need to provide an opt out notice to consumers, and (iii) will not need to implement procedures to honor the wishes of consumers that choose to opt out of certain information sharing.

--Whether the bank already has a notice describing its privacy policy. 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 revising that policy to comply with the regulation are likely to be significantly less than would be the costs for those institutions having to develop a new policy.

--Whether the bank already has an opt-out mechanism in place pursuant to the Fair Credit Reporting Act (FCRA). Under the FCRA, a bank must provide opt out notices and have an opt out mechanism in place if the bank (i) shares certain consumer information (i.e., application or credit report information) with its affiliates, and (ii) does not want to be treated as a consumer reporting agency under the Act. A bank that already gives FCRA notices and wants to share nonpublic personal information with nonaffiliated third parties should be able to adapt its existing opt out mechanism to accommodate the requirements of the final rule.

D. Summary of Significant Issues Raised by the Public Comments; Description of Steps the Agency Has Taken to Minimize Burden

One approach to minimizing the burden on small entities would be to provide a specific

exemption for such institutions. The OCC has no authority under the statute to grant an exception that would remove small institutions from the entire scope of the rule. The OCC does have exemptive authority under section 504(b) to grant such exceptions to the opt out provisions "as are deemed consistent with the purposes of" the statute. The OCC believes that a wholesale exemption for small banks from the opt out provisions would be inconsistent with the purposes of the Act. 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 the privacy of someone's nonpublic personal information is no less deserving of protection simply because the information is obtained by a small bank.

The final rule does, however, provide substantial flexibility so that any bank, regardless of size, may tailor its practices to its individual needs. For example, to minimize the burden and costs of distributing privacy policies, the final rule (i) allows each bank to choose the method by which it will distribute required notices (e.g., banks may include an annual privacy notice with periodic account statements that the bank already sends to the customer) and (ii) allows for the initial privacy notice to be provided with other Federally mandated consumer disclosures, such as those required under the Truth-in-Lending Act.

In addition, the OCC carefully considered comments that suggested a variety of other alternatives to reduce burden. In response to these comments, the agency attempted to minimize the burden on all businesses, including small entities, in a manner consistent with providing the privacy protections mandated by the Act. The discussion below reviews some of the changes adopted in the

final rule to accomplish this purpose. For a more complete discussion of significant issues raised by public comments and the changes adopted in the final rule, see the section-by-section analysis above, which is incorporated herein by reference (Supplementary Information, part III).

Content of Disclosures. Many commenters interpreted the rule as requiring long, detailed privacy disclosures that, in these commenters' view, would be of little benefit to consumers. To address these comments, the final rule clarifies the level of detail that the OCC believes is appropriate under the statute. In particular, the final rule substantially revises the examples of disclosures that would satisfy the rule; Appendix A includes sample clauses that might be used; and the preamble states that the Agencies believe disclosures required by the rule could fit on a typical tri-fold brochure. Also, the Agencies have provided additional guidance under the caption Guidance for Certain Financial Institutions (Guidance) (Supplementary Information, Part IV). This Guidance, as well as the sample clauses in Appendix A, are intended to minimize the burden and costs for all banks, particularly small banks that will not generally be sharing nonpublic personal information with nonaffiliated third parties (except pursuant to the exceptions). In addition, the final rule permits a bank to provide a short-form privacy notice to a consumer that does not become a customer, provided the bank gives the consumer an opt out notice and notifies the consumer of a reasonably convenient method by which to obtain a copy of the full privacy notice.

Definition of Nonpublic Personal Information. A bank that wants to share nonpublic personal information about a consumer with a nonaffiliated third party generally must comply with the opt out restrictions in the rule. However, information that is considered “publicly available information” is excluded from the definition of nonpublic personal information. The proposed rule offered two

alternatives. Under Alternative A, information that is generally available from a public source would not be considered "publicly available information" unless a bank actually obtains the information from a public source. Under Alternative B, the fact that the information could be obtained from a public source is sufficient for the information to be considered publicly available. For the reasons stated earlier in the preamble, the OCC adopted a slightly revised version of Alternative B, the less burdensome option.

Effective Date. By operation of section 510 of the statute, the relevant provisions of Title V take effective November 12, 2000. However, the statute authorizes the agencies to prescribe a later date if implementing regulations are adopted. The proposed rule used the effective date prescribed by the statute. The OCC received a large number of comments from banks, including many from small entities, that requested more time to comply. Many such comments suggested that overall compliance costs could be reduced by delaying the effective date. For the reasons stated earlier in the preamble, the OCC believes it would be appropriate to give banks until July 1, 2001, to comply with the rule.

New Notices Not Required for Each New Financial Product or Service. Some banks, including small entities, expressed concern that the proposed rule may require a new initial notice each time a consumer obtains a new financial product or service. This would be especially burdensome for banks that adopt a universal privacy policy that covers multiple products and services. To address these concerns and minimize economic burden, the final rule clarifies that a new initial notice is not required if the bank has given the customer the bank's initial notice, and that the bank's initial notice remains accurate with respect to the new product or service.

Annual Notice Requirement. Many banks, including small entities, suggested alternative, less

burdensome methods for complying with the requirement that banks provide their customers with an annual privacy notice. As discussed earlier in the preamble, the OCC responded to these comments with a provision in the final rule that permits a bank to comply with the annual privacy notice requirements for customers under certain circumstances by continually posting the notice on the bank's web site in a clear and conspicuous manner.

Notice to Joint Account Holders. As noted earlier in the preamble, the final rule allows banks to provide one notice to joint account holders, with the understanding being that a decision to opt out made by one of the account holders will, absent a provision in the opt out notice to the contrary, prevent the bank from disclosing any nonpublic personal information about any of the account holders. This is particularly advantageous for banks, including small entities, that do not intend to share nonpublic personal information with nonaffiliated third parties (except as permitted under the exceptions).

Board: The Regulatory Flexibility Act (5 U.S.C. 604) requires an agency to publish a final regulatory flexibility analysis when promulgating a final rule that was subject to notice and comment.

Need for and objectives of rule. As discussed above, this rule implements the privacy provisions in sections 502-510 of the GLB Act. The rule's objectives are to protect nonpublic personal information about consumers collected by financial institutions by:

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

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

(3) Providing 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 certain exceptions.

Comments on the initial regulatory flexibility analysis. Although few commenters addressed the initial regulatory flexibility analysis specifically, many commenters addressed the regulatory burdens that were discussed in that analysis. Commenters provided a wide range of estimates of the costs of compliance, demonstrating the difficulty of precisely measuring the implementation costs for GLB Act privacy provisions. For example, one commenter representing a $4 billion dollar multi-bank holding company with ten financial institutions, estimated compliance costs at $160,000/year (an average of $16,000 per institution), contrasted with a $500 million dollar institution that estimated compliance costs at $40,000/year. Another commenter representing an $18 billion dollar bank holding company estimated compliance costs at $2.1 million, while one of the nation's largest financial institutions estimated compliance costs between $2.5-$18 million. In another comment, a public policy group estimated that the costs of the rule "may likely exceed $223 million annually" based on a sample of deposit accounts and estimated loan accounts at 54 "major institutions" around the United States.

The most significant comments on burden discussed the rule's effective date and the amount of detail that financial institutions would have to provide in their initial and annual notices.

Many commenters urged the Board to extend the proposed November 12, 2000, effective date, for periods ranging from six months to two years. Most of these commenters argued that complying with the rule by November 12, 2000, would place an extraordinary burden on their businesses, particularly because the notices required by the rule would mandate changes to computer software, employee training, and compliance systems. To address these concerns, compliance with the

final rule will be deferred until July 1, 2001.

Many commenters urged the Board to reduce the level of detail that they perceived would be required in the notices under the proposed rule. Commenters argued, for instance, that requiring a detailed description of all of the sources of information that they use to collect information about their customers would make the notices too lengthy and complicated. In a similar vein, many commenters proposed that the Board should issue model forms to demonstrate the kinds of notices that would be permitted by the rule.

The Board believes that the intent of the original proposal on the level of detail expected under the proposed rule was widely misinterpreted. The notices section has been redrafted in an effort to clarify the requirements. This should lead to modular provisions based on examples in the regulations that could be used by most institutions. The Board and the other Agencies have included, in an appendix to the final rule, sample clauses illustrating elements of the notice requirements for a small institution that does not sell information for marketing purposes and a large holding company with multiple affiliates that distributes information broadly. The Board and the other Agencies have also includes a guide to compliance for the small institutions as supplementary information in the Federal Register notice.

Nevertheless, some institutions may have to craft notice provisions to cover unique aspects of their privacy practices. This is necessary because it is impossible for agency staff to anticipate all disclosure practices. In the absence of knowledge of these practices, any attempt to craft “model notices” that could be used by all institutions runs a substantial risk of being misleading.

The Board also modified the final rule to clarify that a financial institution need not provide

another initial notice to an existing customer who obtains a new financial product or service so long as the previous notice provided to that customer was accurate with respect to the new financial product or service. The Board believes that this provision will enable a financial institution to adopt a single, comprehensive privacy policy for a its financial products and services, and at the same time, reduce the costs to ensure that it delivers an accurate copy of its policy to each customer.

Institutions covered. The Board's final rule will apply to approximately 9,500 institutions, including 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. The Board estimates that over 4,500 of the institutions are small institutions with assets less than $100 million.

New compliance requirements. The final 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.

Minimizing impact on 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 its customers. 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 that one of the purposes of the Act is to provide notice about the disclosure 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. To aid these institutions in complying with the rule, the Board and the other Agencies have included guidance for certain institutions in this Federal Register notice and have included, as an appendix to the final rule, sample clauses that institutions may use in drafting their notices.

FDIC: The Regulatory Flexibility Act (5 U.S.C. 601-612) (RFA) requires, subject to certain exceptions, that federal agencies prepare an initial regulatory flexibility analysis (IRFA) with a proposed rule and a final regulatory flexibility analysis (FRFA) with a final rule, unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities.[15] At the time

---

[15] 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.

of issuance of the proposed rule, the FDIC could not make such a determination for certification, therefore the FDIC issued an IRFA pursuant to section 603 of the RFA. After considering the comments submitted in response to the proposed rule, the FDIC believes that it does not have sufficient information to determine whether the final rule would have a significant economic impact on a substantial number of small entities. Therefore, pursuant to section 604 of the RFA, the FDIC provides the following FRFA.

This FRFA incorporates the FDIC's initial findings, as set forth in the IRFA; addressees the comments submitted in response to the IRFA; and describes the steps the FDIC has taken in the final rule to minimize the impact on small entities, consistent with the objectives of the GLB Act. Also, in accordance with Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104-121), the FDIC will in the near future issue a Small Entity Compliance Guide to assist small entities in complying with this rule.

Statement of the Need/Objectives of the Rule

The final rule implements the provisions of Title V, Subtitle A of the GLB 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 institutions from sharing nonpublic personal information about consumers with nonaffiliated third parties, and permit consumers to prevent institutions from disclosing nonpublic personal information about them to certain non-affiliated third parties by "opting out" of that disclosure. Section 504 of the GLB Act requires the FDIC, in

consultation with representatives of State insurance authorities, to prescribe "such regulations as may be necessary" to carry out the purposes of Title V, Subtitle A. If no regulations were promulgated, substantive burdens imposed by the Act (e.g., the notice, information sharing restrictions, and opt out requirements) would have become effective and binding on banks one year from the date the Act was signed into law. The FDIC believes that the final rule gives the private sector greater certainty on how to comply with the statute and clearer guidance regarding how it will be enforced.

Summary of Significant Issues Raised in Public Comments

In the IRFA, the FDIC specifically requested information on the costs of creating privacy policy disclosures, distributing privacy policy disclosures, implementing "opt out" disclosure and processing requirements, and complying with the proposed rule in its entirety. The FDIC received few comments responsive to the issue of implementation costs. While the majority of commenters representing the financial services industry indicated that compliance with the regulation would require significant effort, these comments most often requested additional time to comply with the final rule, and did not address estimated costs to comply with the regulation.

The few comments that the FDIC did receive quantifying the economic costs of compliance reflected a wide range of estimates, demonstrating the difficulty of precisely measuring the implementation costs for GLB Act privacy provisions. For example, one commenter representing a $4 billion dollar multi-bank holding company with ten financial institutions, estimated compliance costs at $160,000/year (an average of $16,000 per institution), contrasted with a $500 million dollar institution that estimated compliance costs at $40,000/year. Another commenter representing an $18 billion dollar bank holding company estimated compliance costs at $2.1 million, while one of the nation's

largest financial institutions estimated compliance costs between $2.5-$18 million. In another comment, a public policy group estimated that the costs of the rule "may likely exceed $223 million annually" based on a sample of deposit accounts and estimated loan accounts at 54 "major institutions" around the United States[16].

Summary of the Agency Assessment of Issues Raised in Public Comments

Both the limited numbers of comments received that discussed compliance costs and the wide range of estimates provided, reflect the uncertainty of estimating the costs of implementing the GLB Act requirements. The new compliance requirements will indeed create additional economic costs for institutions, especially those that disclose information to nonaffiliated third parties. These costs include, but are not limited to (1) reviewing current information sharing practices; (2) determining operational changes necessary; (3) identifying sources/uses of customer information; (4) preparing disclosure forms; and (5) training staff. Most, if not, all of these costs result from requirements expressly mandated by the GLB Act.

After a careful review of the comments received, the FDIC does not have a practicable or reliable basis for quantifying the costs of implementing the requirements of the GLB Act. We expect that compliance costs will vary significantly between institutions depending on information sharing practices. The FDIC continues to believe that the costs of implementing the opt out provisions of the final rule will be insubstantial for financial institutions that only disclose nonpublic personal information

[16] This estimate was not limited to FDIC-supervised institutions, but rather was based on all financial institutions subject to the GLB Act.

about consumers to nonaffiliated third parties pursuant to the exceptions provided under Sections 332.14 and 332.15. FDIC's determination is based on the observations of FDIC examiners, which were discussed in the IRFA, and the analysis of comments received in response to the proposed rule. These institutions may provide relatively simple initial and annual notices to consumers with whom they establish customer relationships. However, the FDIC cannot determine either the number or identity of institutions that will not disclose nonpublic personal information about consumers to nonaffiliated third parties.

Description/Estimate of Small Entities to which the Rule will Apply

The final rule will apply to approximately 3,700 FDIC-insured State nonmember banks that are small entities (assets less than $100 million) as defined by the RFA.

Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

The final rule contains new compliance requirements for all covered institutions, most of which are required by the GLB 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. As discussed earlier, the FDIC does not have a practicable or reliable basis for quantifying the compliance costs of

the final rule. Nor can the FDIC determine the number of small entities that will disclose nonpublic personal information about consumers to nonaffiliated third parties.

Steps Agency has taken to Minimize the Significant Economic Impact on Small Entities

The final rule incorporates new compliance requirements, which are expressly mandated by the GLB Act. The GLB Act mandates (1) providing notice of privacy policies/practices; (2) restricting the conditions under which a financial institution may disclose nonpublic personal information to nonaffiliated third parties; and (3) providing a method for consumers to prevent their nonpublic personal information from being shared with nonaffiliated third parties. The FDIC has sought to minimize the burden on all businesses, including small entities, in promulgating this final rule. Nonetheless, the statute does not authorize the FDIC to create exemptions from the GLB Act based on an institution's size. While the final rule attempts to clarify, consolidate, and simplify the statutory requirements for all entities, the FDIC has little discretion, if any, to mandate different compliance standards for small entities. Moreover, different compliance standards would be inconsistent with the purposes of GLB Act.

Throughout this rulemaking proceeding, the FDIC sought to gather information regarding the economic impact of the GLB Act's requirements for all financial institutions, including small entities. The proposed rule and the IRFA included a number of questions for public comment regarding the costs associated with complying with the rule and the impact on small entities. In addition, the FDIC held a public forum on privacy[17] during the comment period, which included representatives of small insured depository institutions and topics designed to elicit information about the rule's economic

[17] FDIC Forum, "Consumer Privacy in the Financial Services Industry. March 23, 2000.

impact. The FDIC carefully considered comments that suggested a variety of alternatives that could minimize the economic and overall burden of complying with the final rule. The discussion below reviews some of the significant changes adopted in the final rule to accomplish this purpose. For a more complete discussion of the changes adopted in the final rule, see the "Section-by-section analysis" under Supplementary Information**,** Part III.

1. Sample Disclosure Clauses (Appendix A to Part 332) and Guidance for Certain Institutions (Supplementary Information, Part IV).

Many commenters expressed concern over the amount of detail that appears to be required in both initial and annual Notices. In addition many of the commenters requested model forms for guidance as to the level of detail required. The FDIC did not intend for the disclosures to be overly detailed and thus, burdensome for institutions and potentially overwhelming for consumers. In response to these comments, Appendix A to Part 332 contains sample clauses to clarify the level of detail that the FDIC believes is necessary and appropriate to be consistent with the statute. The FDIC has also provided additional assistance under the caption Guidance for Certain Institutions (Guidance) (Supplementary Information, Part IV). The Guidance generally clarifies the operation of the final rule. It also provides an example of a notice for small institutions that only share nonpublic personal information with nonaffiliated third parties pursuant to the exceptions provided in Sections 332.14 and 332.15. The Guidance may be used in conjunction with the sample clauses contained in Appendix A.

The sample clauses under Appendix A and the Guidance are intended to minimize the burden and costs to financial institutions, including small entities. This is especially true for small institutions that only share nonpublic personal information with nonaffiliated third parties pursuant to the exceptions

provided in Section 332.14 and 332.15. These institutions may provide relatively simple initial and annual notices to consumers with whom they establish customer relationships.

2. Definition of nonpublic personal information

In the proposed rule, the FDIC provided two alternatives for defining nonpublic personal information. The first, (Alternative A) deemed information as publicly available only if a financial institution actually obtained the information from a public source, whereas the second (Alternative B) treated information as publicly available if a financial institution could obtain it from such a source. A significant majority of commenters favored Alternative B. Many commenters suggested that implementing Alternative A would be overly burdensome. Institutions would have to develop some sort of methodology to distinguish between information obtained from consumers, versus information obtained through public sources. In response to these comments, the final rule adopts a modified version of Alternative B (refer to Section-by-section analysis for additional information) that treats information as publicly available if a financial institution could obtain the information from a public source. The final rule addresses the concerns of financial institutions—including small institutions—by adopting the least economically burdensome definition of nonpublic personal information.

3. Effective Date

Section 510 of the GLB 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, i.e., November 12, 2000. However, section 510(1) authorizes the Agencies to prescribe a later date in the rules enacted pursuant to section 504. The proposed rule sought comment on the effective date prescribed by the statute. The overwhelming majority of commenters requested additional time to comply with the final rule.

Several commenters noted that financial institutions may encounter difficulty managing the expenses and resources required to comply with the final rule as the institution's budget for the current year was established prior to the issuance of the proposed regulation. This may be especially true for small institutions that face already tight budgetary constraints due to heightened competition. In response to these concerns, the FDIC has retained the effective date of November 13, 2000, but, in order to provide sufficient time for institutions to establish policies and systems to comply with the requirements of this part, the FDIC has extended the time for compliance with this part until July 1, 2000. This additional time will allow institutions to properly budget for any necessary expenses and staff resources required to comply with this rule and to make all necessary operational changes.

4. New notices not required for each new financial product or service

Some commenters expressed concern that the proposed rule may require a new initial notice each time a consumer obtains a new financial product or service. This would be especially burdensome for institutions that adopt a universal privacy policy that covers multiple products and services. To address these concerns and minimize economic burden, the final rule was clarified to instruct institutions that a new initial notice is not required if the institution has given the customer the institution's initial notice, and that the institution's initial notice remains accurate with respect to the new product or service.

5. Short form Initial Notice for Consumers

In the proposed rule, institutions were required to provide consumers a copy of a financial institution's complete initial notice when there is no customer relationship. In response to comments that suggested that the objectives of the initial notice requirements of the statute could be accomplished

in a less burdensome way, the FDIC has exercised its exemptive authority as provided in section 504(b) to create an exception to the general rule that otherwise requires a financial institution to provide both the initial and opt out notices to a consumer before disclosing nonpublic personal information about that consumer to nonaffiliated third parties. A financial institution may provide a "short-form" initial notice along with the opt out notice to a consumer with whom the institution does not have a customer relationship. This short-form notice must state that the disclosure containing information about the institution's privacy policies and practices is available upon request and provide one or more reasonable means by which the consumer may obtain a copy of the notice. This provision in the final rule will lessen the burden on financial institutions, including small entities.

6. Notice to Joint Account Holders.

As noted earlier in the preamble, the final rule allows institution's to provide one notice to joint account holders, with the understanding being that a decision to opt out made by one of the account holders will, absent a provision in the opt out notice to the contrary, prevent the institution from disclosing any nonpublic personal information about any of the account holders. This is particularly advantageous for institutions, including small entities, that do not intend to share nonpublic personal information with nonaffiliated third parties (except as permitted under the exceptions).

OTS:

C. Executive Order 12866

OCC: The Comptroller of the Currency has determined that this 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 GLB Act. Since, the GLB 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 GLB 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.

For a financial institution that does not intend to disclose nonpublic personal information about its consumers or customers to nonaffiliated third parties, the burden created by the statute and implementing regulation is that of preparing and distributing an initial and annual notice of the institution's privacy policies and practices. The institution need not provide an opt out notice or establish a system for consumers to opt out. For institutions that do intend to make such disclosures, they will do so only after determining that the benefits of making the disclosures of nonpublic personal information outweigh the costs. Accordingly, the regulation's provisions governing opt outs impose no net burden on those institutions disclosing nonpublic personal information. The final rule makes a large number of significant changes to the requirements governing initial and annual notices that reduce burden while preserving the consumer protections created by the statute.

OTS:

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 rule's provisions are already mandated by the applicable provisions in Title V of the GLB Act, which would become effective and binding on the private sector even without a regulatory promulgation. Therefore, the OCC and OTS have determined that this 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.

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 amends 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.

Subpart A–Privacy and Opt Out Notices

40.4 Initial privacy notice to consumers required.

40.5 Annual privacy notice to customers required.

40.6 Information to be included in privacy notices.

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

40.8 Revised privacy notices.

40.9 Delivering privacy and opt out notices.

Subpart B–Limits on Disclosures

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

40.11 Limits on redisclosure and reuse of information.

40.12 Limits on sharing account number information for marketing purposes.

Subpart C–Exceptions

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

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

40.15 Other exceptions to notice and opt out requirements.

Subpart D–Relation to Other Laws; Effective Date

40.16 Protection of Fair Credit Reporting Act.

40.17 Relation to State laws.

40.18 Effective date; transition rule.

Appendix A to Part 40–Sample Clauses

Authority: 12 U.S.S. 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 customers about its privacy policies and practices;

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

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

(b) Scope. This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the

institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to United States offices of entities for which the Office of the Comptroller of the Currency has primary supervisory authority. They are referred to in this part as "the bank." These are national banks, 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. Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-1320d-8).

§ 40.2 Rule of construction.

The examples in this part and the sample clauses in Appendix A of this part are not exclusive. Compliance with an example or use of a sample clause, 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 in the notice.

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

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

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

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

(D) Avoids multiple negatives;

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

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

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

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

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

(C) Provides wide margins and ample line spacing;

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

(E) In a form that combines the bank's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(g) Control of a company means:

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

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

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

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

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

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

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

(B) Obtains a loan from the bank;

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

(D) Purchases an insurance product from the bank;

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

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

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

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

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

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

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

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

(j) Federal functional regulator means:

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

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

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

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

(5) The National Credit Union Administration Board; and

(6) The Securities and Exchange Commission.

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

(2) Financial institution does not include:

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

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

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

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

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

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

(i) A bank's affiliate; or

(ii) A person employed jointly by a bank and any company that is not the bank's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

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

(n) (1) Nonpublic personal information means:

(i) Personally identifiable financial information; and

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

(2) Nonpublic personal information does not include:

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

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

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

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

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

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

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

(iii) The bank otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.

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

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

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

(C) The fact that an individual is or has been one of the bank's customers or has obtained a financial product or service from the bank;

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

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

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

(G) Information from a consumer report.

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

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

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

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

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

(ii) Widely distributed media; or

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

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

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

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

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

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

(iii) Reasonable basis. (1) A bank has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the bank has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

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

Subpart A–Privacy and Opt Out Notices

§ 40.4 Initial privacy notice to consumers required.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(A) Originates the loan to the consumer; or

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

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

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

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

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

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

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

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

(ii) Substantial delay of customer's transaction. Providing notice not later than when a bank establishes a customer relationship would substantially delay the customer's transaction when:

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

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

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

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

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

§ 40.5 Annual privacy notice to customers required.

(a)(1) General rule. A bank must provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. A bank may define the 12-consecutive-month period, but the bank must apply it to the customer on a consistent basis.

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

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

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

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

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

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

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

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

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

§ 40.6 Information to be included in privacy notices.

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

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

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

(3) The categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information, other than those parties to whom the bank discloses information under §§ 40.14 and 40.15;

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

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

(6) An explanation of the consumer's right under § 40.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

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

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

(9) Any disclosure that the bank makes under paragraph (b) of this section.

(b) Description of nonaffiliated third parties subject to exceptions. If a bank discloses nonpublic personal information to third parties as authorized under §§ 40.14 and 40.15, 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 required to state only that it makes disclosures to other nonaffiliated third parties as permitted by law.

(c) Examples. (1) Categories of nonpublic personal information that the bank collects. A bank satisfies the requirement to categorize the nonpublic personal information that it collects if it lists the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with the bank or its affiliates;

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

(iv) Information from a consumer reporting agency.

(2) Categories of nonpublic personal information the bank discloses. (i) A bank satisfies the requirement to categorize the nonpublic personal information that it discloses if the bank lists the categories described in paragraph (e)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.

(ii) If a bank reserves the right to disclose all of the nonpublic personal information about consumers that it collects, it may simply state that fact without describing the categories or examples of the nonpublic personal information it discloses.

(3) Categories of affiliates and nonaffiliated third parties to whom the bank discloses. A bank satisfies the requirement to categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic personal information if the bank lists the following categories, as applicable, and a few examples to illustrate the types of third parties in each category:

(i) Financial service providers;

(ii) Non-financial companies; and

(iii) Others.

(4) Disclosures under exception for service providers and joint marketers. If a bank discloses nonpublic personal information under the exception in § 40.13 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the bank satisfies the disclosure requirement of paragraph (a)(5) of this section if it:

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

(ii) States whether the third party is:

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

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

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

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

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

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

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

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

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

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

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

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

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

(ii) For a consumer who conducts business in person at the bank's office, maintain copies of the notice on hand that the bank provides to the consumer immediately upon request.

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

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

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

(f) Sample clauses. Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this part.

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

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

(i) That the bank discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

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

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

(2) Examples. (i) Adequate opt out notice. A bank provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the bank:

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

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

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

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

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

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

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

(iii) Unreasonable opt out means. A bank does not provide a reasonable means of opting out if:

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

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

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

(b) Same form as initial notice permitted. A bank may provide the opt out notice together with or on the same written or electronic form as the initial notice the bank provides in accordance with § 40.4.

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

(d) Joint relationships. (1) If two or more consumers jointly obtain a financial product or service from a bank, the bank may provide a single opt out notice. The bank's opt out notice must explain how the bank will treat an opt out direction by a joint consumer (as explained in paragraph (d)(5) of this section).

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

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

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

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

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

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

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

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

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

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

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

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

(e) Time to comply with opt out. A bank must comply with a consumer's opt out direction as soon as reasonably practicable after the bank receives it.

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

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

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that the bank collected during or related to that relationship.

If the individual subsequently establishes a new customer relationship with the bank, the opt out direction that applied to the former relationship does not apply to the new relationship.

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

§ 40.8 Revised privacy notices.

(a) General rule. Except as otherwise authorized in this part, a bank must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the bank provided to that consumer under § 40.4, unless:

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

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

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

(4) The consumer does not opt out.

(b) Examples. (1) Except as otherwise permitted by §§ 40.13, 40.14, and 40.15, a bank must provide a revised notice before it:

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

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

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

(2) A revised notice is not required if the bank discloses nonpublic personal information to a new nonaffiliated third party that the bank adequately described in its prior notice.

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

§ 40.9 Delivering privacy and opt out notices.

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

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

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

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

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

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

(2) Examples of unreasonable expectation of actual notice. A bank may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

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

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

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

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

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

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

(e) Retention or accessibility of notices for customers. (1) For customers only, a bank must provide the initial notice required by § 40.4(a)(1), the annual notice required by § 40.5(a), and the revised notice required by § 40.8 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) Examples of retention or accessibility. A bank provides a privacy notice to the customer so that the customer can retain it or obtain it later if the bank:

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

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

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

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

Subpart B–Limits on Disclosures

§ 40.10 Limits on disclosure of non-public personal information to nonaffiliated third parties.

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

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

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

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

(iv) The consumer does not opt out.

(2) Opt out definition. Opt out means a direction by the consumer that the bank not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 40.13, 40.14, and 40.15.

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

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

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

(iii) Isolated transaction with consumer. For an isolated transaction, such as the purchase of a cashier's check by a consumer, a bank provides the consumer with a reasonable opportunity to opt out if the bank provides the notices required in paragraph (a)(1) of this section at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

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

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

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

§ 40.11 Limits on redisclosure and reuse of information.

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

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

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

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

(2) Example. If a bank receives a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in § 40.14(a), the bank may disclose that information under any exception in §§ 40.14 or 40.15 in the ordinary course of business in order to provide those services. For example, the bank could disclose the information in response to a properly

authorized subpoena or to its attorneys, accountants, and auditors. The bank could not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.

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

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

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

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

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

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

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

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

(1) The third party may disclose the information to the bank's affiliates;

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

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

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

(1) To the bank's affiliates;

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

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

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

(a) General prohibition on disclosure of account numbers. A bank must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar

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

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

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

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

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

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

Subpart C–Exceptions

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

(a) General rule. (1) The opt out requirements in §§ 40.7 and 40.10 do not apply when a bank provides nonpublic personal information to a nonaffiliated third party to perform services for the

bank or functions on the bank's behalf, if the bank:

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

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

(2) Example. If a bank discloses nonpublic personal information under this section to a financial institution with which the bank performs joint marketing, the bank's contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in §§ 40.14 or 40.15 in the ordinary course of business to carry out that joint marketing.

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

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

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

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

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

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

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

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

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

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

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

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

(iii) To provide a confirmation, statement, or other record of the transaction, or information on

the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;

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

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

(vi) In connection with:

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

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

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

§ 40.15 Other exceptions to notice and opt out requirements.

(a) Exceptions to opt out requirements. The requirements for initial notice to consumers in § 40.4(a)(2), the opt out in §§ 40.7 and 40.10, and service providers and joint marketing in § 40.13 do not apply when a bank discloses nonpublic personal information:

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

revoked the consent or direction;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Subpart D–Relation to Other Laws; Effective Date

§ 40.16 Protection of Fair Credit Reporting Act.

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

section 603 of that Act.

§ 40.17 Relation to State laws.

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

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

§ 40.18 Effective date; transition rule.

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

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

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

customers and has mailed the initial notice to all the bank's existing customers.

(c) Two-year grandfathering of service agreements. Until July 1, 2002, a contract that a bank has entered into with a nonaffiliated third party to perform services for the bank or functions on the bank's behalf satisfies the provisions of § 40.13(a)(2) of this part, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the bank entered into the agreement on or before July 1, 2000.

APPENDIX A TO PART 40–SAMPLE CLAUSES

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

A-1–Categories of information a bank collects (all institutions)

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

Sample Clause A-1:

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

• Information we receive from you on applications or other forms;

• Information about your transactions with us, our affiliates, or others; and

• Information we receive from a consumer reporting agency.

A-2–Categories of information a bank discloses (institutions that disclose outside of the exceptions)

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

Sample Clause A-2, Alternative 1:

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

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

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

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

Sample Clause A-2, Alternative 2:

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

A-3–Categories of information a bank discloses and parties to whom the bank discloses (institutions that do not disclose outside of the exceptions)

A bank may use this clause, as applicable, to meet the requirements of §§ 40.6(a)(2), (3), and

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

Sample Clause A-3:

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

A-4–Categories of parties to whom a bank discloses (institutions that disclose outside of the exceptions)

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

Sample Clause A-4:

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

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

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

• Others, such as [provide illustrative examples, such as “non-profit organizations”].

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

A-5–Service provider/joint marketing exception

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

Sample Clause A-5, Alternative 1:

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

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

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

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

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice,

such as “above” or “below”] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt out right (institutions that disclose outside of the exceptions)

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

Sample Clause A-6:

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

A-7–Confidentiality and security (all institutions)

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

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as “those employees who need to know that information to provide products or

services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

[This signature page relates to the joint final rule “Privacy of Consumer Financial Information," 12 CFR Part 40, Docket No. 00-XX]

Date	John D. Hawke, Jr. Comptroller of the Currency