

Compliance for Deposit Operations

Regulation P: Privacy of Consumer Financial Information

Pennsylvania Association of Community Bankers

November 2020

This publication is designed to provide information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a professional competent in the area of special need should be sought.

© Copyright 2020
Young & Associates, Inc.
All rights reserved



Consultants to the Financial Industry

Young & Associates, Inc.

121 E. Main Street
P.O. Box 711
Kent, OH 44240

Phone: 330.678.0524
Fax: 330.678.6219
www.younginc.com

Table of Contents

| | |
|--|----|
| Section 1: Privacy – Purpose and Scope [12 C.F.R. § 1016.1] Model Privacy Forms and Examples [12 C.F.R. § 1016.2]..... | 1 |
| Section 2: Selected Definitions [12 C.F.R. § 1016.3] | 4 |
| Section 3: What is Protected? [12 C.F.R. § 1016.3]..... | 8 |
| Section 4: Recipients of Privacy Notices [12 C.F.R. § 1016.3] | 13 |
| Section 5: Initial Privacy Notice [12 C.F.R. § 1016.4] | 17 |
| Section 6: Annual Privacy Notice [12 C.F.R. § 1016.5] | 22 |
| Section 7: Privacy Notice Contents [12 C.F.R. § 1016.6] | 26 |
| Section 8: Opt-Out Requirements [12 C.F.R. § 1016.7]..... | 33 |
| Section 9: Notice to Customers: Revised Privacy Notice [12 C.F.R. § 1016.8] | 40 |
| Section 10: Delivery of Notices [12 C.F.R. § 1016.9]..... | 42 |
| Section 11: Limits on Disclosures [12 C.F.R. § 1016.10]..... | 46 |
| Section 12: Limits on Redisclosure and Reuse [12 C.F.R. § 1016.11] | 49 |
| Section 13: Limits on Sharing Account Number Information for Marketing Purposes [12 C.F.R. § 1016.12] | 53 |
| Section 14: Exceptions [12 C.F.R. § 1016.13]..... | 55 |
| Section 15: Exceptions [12 C.F.R. § 1016.14]..... | 57 |
| Section 16: Exceptions [12 C.F.R. § 1016.15]..... | 60 |
| Section 17: Relation to Other Laws [12 C.F.R. § 1016.16] and [12 C.F.R. § 1016.17] | 63 |
| Section 18: The Model Privacy Forms – Appendix A | 64 |
| Section 19: The Model Privacy Forms – Appendix B | 67 |
| Section 20: The Model Privacy Forms – Appendix C | 69 |

Section 1: Privacy – Purpose and Scope [12 C.F.R. § 1016.1]

Model Privacy Forms and Examples [12 C.F.R. § 1016.2]

Introduction

This manual contains all relevant regulatory text. Some regulatory text has been omitted, as it is not pertinent for financial institutions. We have indicated where those omissions were made. The regulation has no commentary. Words that appear in **bold** are only to assist the reader in finding information on the page.

Purpose and Scope [12 C.F. R. § 1016.1]

Regulatory Discussion

The regulation applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes, and requires the bank to:

- Provide notice to customers about its privacy policies and practices;
- Describe the conditions under which the bank may disclose nonpublic information about consumers to nonaffiliated third-parties; and
- Provide a method for consumers to prevent the bank from disclosing that information to nonaffiliated third-parties by “opting out” of that disclosure, subject to certain exceptions.

The regulation does not apply to companies or individuals who obtain financial products or services for business, commercial, or agricultural purposes.

Neither the law nor the regulations dictate the bank’s policy regarding privacy. That is determined by the bank’s board of directors. Therefore, senior management and the board of directors must make appropriate decisions concerning the bank’s policy.

Regulatory Text

(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 §§1016.13, 1016.14, and 1016.15.

(b) Scope.

- (1) This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to those financial institutions and other persons for which the Bureau of Consumer Financial Protection (Bureau) has rulemaking authority pursuant to section 504(a)(1)(A) of the Gramm-Leach-Bliley Act (GLB Act) (15 U.S.C. 6804(a)(1)(A)). Specifically, this part applies to any financial institution and other covered person or service provider that is subject to Subtitle A of Title V of the GLB Act, including third parties that are not financial institutions but that receive nonpublic personal information from financial institutions with whom they are not affiliated. This part does not apply to certain motor vehicle dealers described in 12 U.S.C. 5519 or to entities for which the Securities and Exchange Commission or the Commodity Futures Trading Commission has rulemaking authority pursuant to sections 504(a)(1)(A)-(B) of the GLB Act (15 U.S.C. 6804(a)(1)(A)-(B)). Except as otherwise specifically provided herein, entities to which this part applies are referred to in this part as “you.”

(2)

- (i) 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).
- (ii) Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution described in §1016.3(l)(3) of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

(3) Nothing in this part shall apply to: [Omitted, as not material to this presentation]

Model Privacy Forms and Examples [12 C.F. R. §1016.2]

Regulatory Discussion

Use of the model privacy form in the Appendix to the regulation, consistent with the instructions in the Appendix, constitutes compliance with the notice content requirements of the regulation, although use of the model privacy form is not required.

Examples

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

Regulatory Text

(a) **Model privacy form.** Use of the model privacy form in the appendix to this part, consistent with the instructions in the appendix constitutes compliance with the notice content requirements of §§1016.6 and 1016.7 of this part, although use of the model privacy form is not required.

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

Section 2: Selected Definitions [12 C.F.R. § 1016.3]

Introduction

General definitions appear in this section. Definitions which are specific to topics which appear later in this manual are included in those sections. We have elected to include the regulatory text in this section without any additional Regulatory Discussion.

Several definitions discuss credit unions and other financial institutions. Readers will note that these portions of the definitions have been removed.

Selected Definitions [12 C.F.R. § 1016.3]

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

(a)

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

(2) **Examples in the case of a credit union.** [Omitted]

(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.** You make your notice reasonably understandable if you:

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

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

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

(D) Avoid multiple negatives;

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

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

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

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

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

(C) Provide wide margins and ample line spacing;

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

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

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

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

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

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

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

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

(g) **Control** of a company means:

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

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

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company as determined by the applicable prudential regulator (as defined in 12 U.S.C. 5481(24)), if any.

(4) **Example in the case of credit unions.** [Omitted]

(h) **Credit union** [Omitted]

(k) **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 National Credit Union Administration Board; and
- (5) The Securities and Exchange Commission.

(l)

- (1) Except for entities described in paragraph (l)(3) of this section, **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) For purposes of paragraph (l)(1) of this section, **financial institution** does not include: [Omitted, as not relevant to this manual]
- (3)
 - (i) Special definition for entities subject to the Federal Trade Commission's enforcement jurisdiction. [Omitted]
 - (ii) [Omitted]
 - (iii) [Omitted]
 - (iv) Examples of entities that are not significantly engaged in financial activities. [Omitted]

(m)

- (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) **Special definition for entities subject to the Federal Trade Commission's enforcement jurisdiction.** [Omitted]

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

(n) **Member** [Omitted]

(o)

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

(i) Your affiliate; or

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

(2) **Nonaffiliated third party** includes, for financial institutions other than credit unions, any company that is an affiliate solely by virtue of your or your affiliate's direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(H) and (I)).

(s)

(1) **You** means a financial institution for which the Bureau has rulemaking authority under section 504(a)(1)(A) of the GLB Act (15 U.S.C. 6804(a)(1)(A)).

(2) **You** does not include: [Omitted]

Section 3: What is Protected? [12 C.F.R. § 1016.3]

Introduction

Generally, nonpublic personally identifiable financial information is protected under this rule. The following definitions include:

- The general definition for personally identifiable financial information, and
- A definition of what personally identifiable financial information is public and nonpublic.

Personally Identifiable Financial Information [12 C.F.R. § 1016.3(q)]

Regulatory Discussion

Includes any of the following:

- Information provided by a consumer to the bank to obtain a financial product or service;
- Information resulting from any transaction involving a financial product or service between the bank and a consumer; or
- Information the bank otherwise obtains about a consumer in connection with providing a financial product or service to that consumer, other than publicly available information.

Examples include:

- Information a consumer provides to the bank on an application to obtain a loan, credit card, or other financial product or service;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- The fact that the individual is or has been a bank customer or has obtained a financial product or service from the bank;
- Other information about a bank's consumer if it is disclosed in a manner that indicates the individual is or has been the bank's consumer;
- Any information that a consumer provides to the bank or that the bank or the bank's agent obtains in connection with collecting on a loan or servicing a loan;
- Any information the bank collects through an Internet "cookie;" or
- Information from a consumer report, such as a credit report.

Does not include:

- A list of names and addresses of customers of an entity that is not a financial institution. For example, the names and addresses of people who subscribe to a particular magazine fall outside the definition. However, if the bank includes those names and addresses as part of a list of the bank's customers, then those names and addresses become nonpublic personal information.
- 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.

Regulatory Text

(q)

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

- (i) A consumer provides to you to obtain a financial product or service from you;
- (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
- (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) **Examples**

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

- (A) Information a consumer provides to you on an application to obtain a loan, a credit card, a credit union membership, or other financial product or service;
- (B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- (C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- (D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- (E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a loan or a credit account;
- (F) Any information you collect through an internet "cookie" (an information collecting device from a Web server); and
- (G) Information from a consumer report.

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

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

Publicly Available Information [12 C.F.R. § 1016.3(r)]

Regulatory Discussion

Includes any information that is lawfully made available to the general public that is obtained from these sources:

- Federal, state, or local government records such as government real estate records and security interest filings.
- Widely distributed media such as from a telephone book, television or radio program, newspaper, or an Internet site that is available to the general public without requiring a password or similar restriction.
- Disclosures to the general public that are required to be made by Federal, state, or local law, such as securities disclosure documents.

Regulatory Text

(r)

- (1) **Publicly available information** means any information that you have 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.** You have a reasonable basis to believe that information is lawfully made available to the general public if you have 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 your consumer has not done so.
- (3) **Examples**
 - (i) **Government records.** Publicly available information in government records includes information in government real estate records and security interest filings.

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

(iii) **Reasonable basis.**

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

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

Nonpublic Personal Information [12 C.F.R. § 1016.3(p)]

Regulatory Discussion

Includes:

- Personally identifiable financial information (see the definition of that term above); and
- 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. For example, 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.

Does not include:

- Any list of individuals' names and addresses that contains only publicly available information;
- Any information that is not derived in whole or part using personally identifiable financial information that is not publicly available; and
- Any information that is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of the bank.

Regulatory Text

(p)

(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 (p)(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.

Section 4: Recipients of Privacy Notices

[12 C.F.R. § 1016.3]

Introduction

Recipients of privacy notices fall into two groups:

1. Consumers
2. Customers

The formal definitions for each of these groups are listed below.

Consumer [12 C.F.R. § 1016.3(e)]

Regulatory Discussion

An individual who obtains or has obtained a financial product or service from the bank that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. **A consumer is an individual who:**

- Applies for credit regardless of whether the credit is extended.
- Provides nonpublic personal information in order to obtain a determination about whether he or she may qualify for a loan, regardless of whether the loan is extended.
- Provides nonpublic personal information in connection with obtaining or seeking to obtain financial, investment, or economic advisory services, regardless of whether an ongoing advisory relationship is established.
- If a bank holds ownership or servicing rights to an individual's loan, 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.

An individual is not a bank's consumer solely because:

- The bank acts as agent for, or provides processing or other services to, another financial institution.
- He or she has designated the bank as trustee for a trust.
- He or she is a beneficiary of a trust for which the bank is a trustee.
- 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.

Regulatory Text

(e)

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

(2) **Examples in the case of a financial institution other than a credit union.** For purposes of this paragraph (e)(2), "you" is limited to financial institutions other than credit unions.

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

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

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

(iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold 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 you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

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

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

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

(3) **Examples in the case of a credit union.** [Omitted]

Customer [12 C.F.R. § 1016.3(i)]

Regulatory Discussion

A customer is a consumer who has a customer relationship with the bank.

Regulatory Text

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

Customer Relationship [12 C.F.R. § 1016.3(i)]

Regulatory Discussion

A continuing relationship between a consumer and the 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. **A consumer has a continuing relationship with the bank if the consumer:**

- Has a deposit or investment account with the bank;
- Obtains a loan from the bank;
- Has a loan for which the bank owns the servicing rights;
- Purchases an insurance product from the bank;
- Holds an investment product through the bank, such as when the bank acts as custodian for securities or assets in an IRA account;
- Enters into an agreement or understanding with the bank whereby the bank undertakes to arrange or broker a home mortgage loan for the consumer;
- Enters into a lease of personal property with the bank; or
- Obtains financial, investment, or economic advisory services from the bank for a fee.

There is not a continuing customer relationship with a bank if:

- The consumer only obtains a financial product or service in an isolated transaction, such as withdrawing cash from the bank's ATM from an account at another financial institution or purchasing a cashier's check or money order.
- The bank sells the consumer's loan and does not retain the right to service the loan.
- The bank sells the consumer airline tickets, travel insurance, or traveler's checks in an isolated transaction.

Regulatory Text

(j)

(1) **Customer relationship** means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. As noted in the examples, and for purposes of this part only, in the case of a credit union, a customer relationship will exist between a credit union and certain consumers that are not the credit union's members.

(2) **Examples in the case of financial institutions other than credit unions and covered entities subject to FTC enforcement jurisdiction.** For purposes of this paragraph (j)(2), “you” is limited to financial institutions other than credit unions and financial institutions described in paragraph (l)(3) of this section.

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

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

(B) Obtains a loan from you;

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

(D) Purchases an insurance product from you;

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

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

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

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

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

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

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

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

(3) **Examples in the case of covered entities subject to FTC enforcement jurisdiction.** [Omitted]

(4) **Examples in the case of a credit union.** [Omitted]

Section 5: Initial Privacy Notice [12 C.F.R. § 1016.4]

General Rule

The regulation requires that the bank provide an initial privacy notice in a “clear and conspicuous” manner [see formal definition, Section 2] that accurately reflects the bank’s privacy policies and practices to its:

- Customers [see formal definition, Section 4], and, potentially,
- Consumers [see formal definition, Section 4].

Timing of the Initial Privacy Notice to New Customers [12 C.F.R. § 1016.4(a) and (c)]

Regulatory Discussion

An initial privacy notice is required to be delivered to new customers:

- At the time a customer relationship is established.
- Exception: The initial notice may be delivered within a reasonable time after the bank establishes a customer relationship provided that the establishing of the customer relationship is not the customer’s election.
- *Example:* the bank acquires the customer’s deposit liability or the servicing rights to his or her loan from another bank and the customer does not have a choice about the acquisition; or
- Providing the notice would substantially delay the customer’s transaction and the customer agrees to receive the notice at a later time.

Example: when 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 the bank establishes a customer relationship with an individual under a program authorized by Title IV of the Higher Education Act of 1965 or similar student loan programs where loan proceeds are disbursed promptly without prior communication between the bank and the customer. However, there would not be a “substantial delay” 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.

Regulatory Text

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

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

(2) *****

(c) When you establish a customer relationship

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

(2) **Special rule for loans.** You establish a customer relationship with a consumer when you originate or acquire the servicing rights to a loan to the consumer for personal, family, or household purposes. If you subsequently transfer the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3) Examples

(i) **Examples of establishing customer relationship by financial institutions other than credit unions and covered entities subject to FTC enforcement jurisdiction.** For purposes of this paragraph (c)(3)(i), “you” is limited to financial institutions other than credit unions and financial institutions described in §1016.3(l)(3). You establish a customer relationship when the consumer:

(A) Opens a credit card account with you;

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

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

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

(ii) **Examples of establishing customer relationship by covered entities subject to FTC enforcement jurisdiction.** [Omitted]

(iii) **Examples of establishing customer relationship by credit unions.** [Omitted]

(iv) **Examples of loan rule.** You establish a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when you:

(A) Originate the loan to the consumer; or

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

Timing of the Initial Privacy Notice to Existing Customers [12 C.F.R. § 1016.4(a) and (c)]

Regulatory Discussion

When an existing customer obtains a new financial product or service from the bank, the initial notice requirements are satisfied when:

- The bank provides a revised privacy notice (see Section 13: Notice to Customers: Revised Privacy Notice) that covers the new financial product or service; or
- The initial, annual, or revised privacy notice that the bank most recently provided to the customer was accurate with respect to the new financial product or service.

Regulatory Text

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

- (1) You may provide a revised privacy notice, under §1016.8 of this part, that covers the customer's new financial product or service; or
- (2) If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

Timing of Initial Privacy Notice to Consumers [12 C.F.R. § 1016.4(b)]

Regulatory Discussion

Prior to disclosing nonpublic information about the consumer to a nonaffiliated third party, unless the disclosure relates to processing and servicing transactions or other miscellaneous exceptions discussed below.

- Exception: The initial notice is not required:
 - If the bank does not disclose nonpublic personal information to a nonaffiliated third party, other than disclosures relating to processing and servicing transactions and other miscellaneous exceptions discussed in “Section 7: Exceptions;” and
 - The bank does not have a customer relationship with the consumer [see formal definition, Section 4].

Regulatory Text

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

(1) *****

(2) **Consumer.** A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§1016.14 and 1016.15 of this part.

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

- (1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§1016.14 and 1016.15; and
- (2) You do not have a customer relationship with the consumer.

Exceptions to the Timing Requirements [12 C.F.R. § 1016.4(e)]

Regulatory Discussion

There can be a delay in the delivery of the notice (still deliver within a reasonable time) if the establishment of the customer relationship is not at the customer's election, such as the purchase of a loan. There can also be a delay if delivery of the notice will unreasonably delay the transaction. Examples of this are below in the regulatory text.

Regulatory Text

(e) Exceptions to allow subsequent delivery of notice.

(1) You may provide the initial notice required by paragraph (a)(1) of this section within a reasonable time after you establish a customer relationship if:

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

(2) Examples of exceptions

(i) Not at customer's election.

(A) In the case of financial institutions other than credit unions and financial institutions described in §1016.3(l)(3), establishing a customer relationship is not at the customer's election if you acquire 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 your acquisition.

(B) [Omitted]

(C) In the case of credit unions [Omitted]

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

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

(B) You establish 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 you and the customer.

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

Delivery of the Initial Privacy Notice [12 C.F.R. § 1016.4(f)]

Regulatory Discussion

All delivery rules are covered in other sections of the regulation.

Regulatory Text

- (f) **Delivery.** When you are required to deliver an initial privacy notice by this section, you must deliver it according to §1016.9 of this part. If you use a short-form initial notice for non-customers according to §1016.6(d) of this part, you may deliver your privacy notice according to §1016.6(d)(3).

Section 6: Annual Privacy Notice [12 C.F.R. § 1016.5]

General Rule and Timing of the Annual Privacy Notice [12 C.F.R. § 1016.5(a)]

Regulatory Discussion

The regulation requires that the bank provide an annual privacy notice in a “clear and conspicuous” manner that accurately reflects the bank’s privacy policies and practices. **This requirement is ONLY for banks that use an opt-out.**

The annual notice must be provided not less than annually during the duration of the customer’s relationship with the bank. Annually means:

- At least once in any period of 12 consecutive months.
- The bank may define the 12-consecutive-month period; however, it must be applied to the customer on a consistent basis.

The bank meets the notice requirement 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 initial notice was provided to the customer.

Example: if a customer opens an account on any day of year one, you must provide an annual notice to that customer by December 31 of year two.

Regulatory Text

(a)

- (1) **General rule.** Except as provided by paragraph (e) of this section, you must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.
- (2) **Example.** You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

Exemption [12 C.F.R. § 1016.5(b) and (c)]

Regulatory Discussion

The bank is not required to provide an annual notice to a former customer. Examples include:

- Deposit accounts which are dormant under the bank's policies;
- Closed-end loan in which:
 - the customer pays the loan in full,
 - the bank charges off the loan, or
 - the bank sells the loan without retaining servicing rights;
- Credit card relationship or other open-end credit relationship when the bank no longer provides statements or notices to the customer or the bank sells the credit card receivables without retaining servicing rights; or
- For other types of relationships, if 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.

Regulatory Text

(b)

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

(2) Examples in the case of financial institutions other than credit unions and covered entities subject to FTC enforcement jurisdiction. For purposes of this paragraph (b)(2), "you" is limited to financial institutions other than credit unions and financial institutions described in §1016.3(l)(3). Your customer becomes a former customer when:

- (i) In the case of a deposit account, the account is inactive under your policies;
- (ii) In the case of a closed-end loan, the customer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;
- (iii) In the case of a credit card relationship or other open-end credit relationship, you no longer provide any statements or notices to the customer concerning that relationship or you sell the credit card receivables without retaining servicing rights; or
- (iv) You have 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.

(3) Examples in the case of covered entities subject to FTC enforcement jurisdiction. [Omitted]

(4) Examples in the case of a credit union. [Omitted]

(c) **Special rule for loans in the case of a financial institution other than a credit union.** If a financial institution other than a credit union does not have a customer relationship with a consumer under the special rule for loans in §1016.4(c)(2) of this part, then it need not provide an annual notice to that consumer under this section.

Delivery of the Annual Privacy Notice [12 C.F.R. § 1016.5(d)]

Regulatory Discussion

This notice must be delivered in writing or electronically (if the customer agrees) so that each consumer can reasonably be expected to receive the actual notice. For further details, delivery instructions are included below.

Regulatory Text

- (d) **Delivery.** When you are required to deliver an annual privacy notice by this section, you must deliver it according to §1016.9 of this part.

Exception [12 C.F.R. § 1016.5(e)]

Regulatory Discussion

This is the most recent section of the regulation. Generally, unless a bank shares information, there is no requirement to provide an annual notice. Once a bank does choose to share (and there is now an opt-out, annual notices are required.

Regulatory Text

(e) Exception to annual privacy notice requirement.

- (1) **When exception available.** You are not required to deliver an annual privacy notice if you:
- (i) Provide nonpublic personal information to nonaffiliated third parties only in accordance with the provisions of §1016.13, §1016.14, or §1016.15; and
 - (ii) Have not changed your policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under §1016.6(a)(2) through (5) and (9) in the most recent privacy notice provided pursuant to this part.
- (2) **Delivery of annual privacy notice after financial institution no longer meets requirements for exception.** If you have been excepted from delivering an annual privacy notice pursuant to paragraph (e)(1) of this section and change your policies or practices in such a way that you no longer meet the requirements for that exception, you must comply with paragraph (e)(2)(i) or (e)(2)(ii) of this section, as applicable.
- (i) **Changes preceded by a revised privacy notice.** If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that §1016.8 requires you to provide a revised privacy notice, you must provide an annual privacy notice in accordance with the timing requirements in paragraph (a) of this section, treating the revised privacy notice as an initial privacy notice.

(ii) **Changes not preceded by a revised privacy notice.** If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that §1016.8 does not require you to provide a revised privacy notice, you must provide an annual privacy notice within 100 days of the change in your policies or practices that causes you to no longer meet the requirements of paragraph (e)(1) of this section.

(iii) **Examples.**

(A) You change your policies and practices in such a way that you no longer meet the requirements of paragraph (e)(1) of this section effective April 1 of year 1. Assuming you define the 12-consecutive-month period pursuant to paragraph (a) of this section as a calendar year, if you were required to provide a revised privacy notice under §1016.8 and you provided that notice on March 1 of year 1, you must provide an annual privacy notice by December 31 of year 2. If you were not required to provide a revised privacy notice under §1016.8, you must provide an annual privacy notice by July 9 of year 1.

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

Section 7: Privacy Notice Contents

[12 C.F.R. § 1016.6]

Contents of Model Notice [12 C.F.R. § 1016.6(a) through (c)(4)]

Regulatory Discussion

The privacy notice must include the following items:

- **The categories of nonpublic personal information that the bank collects.** Only list those that apply:
 - Information from the consumer;
 - Information about the consumer's transactions with the bank or its affiliates;
 - Information about the consumer's transactions with nonaffiliated third parties; and
 - Information from a consumer reporting agency.
- **The categories of nonpublic personal information that the bank discloses (see above).** Only list those that apply, along with a few examples for each category. If the bank reserves the right to disclose all of the nonpublic personal information it collects about consumers, it may simply state that fact without describing the categories or giving examples.
- **The categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic information,** other than those parties to whom the bank discloses information under an exception. Only list those that apply, along with a few examples for each category.
 - Financial service providers;
 - Non financial companies; and
 - Others.
- **The categories of nonpublic personal information about the bank's former customers** that it discloses and the categories of affiliates and nonaffiliated third parties to whom the bank discloses nonpublic information about its former customers, other than those parties to whom the bank discloses information under an exception.
- If the bank **discloses nonpublic personal information to a nonaffiliated third party who is providing services or joint marketing** on the bank's behalf and no other exception applies, a separate description of the categories of nonpublic personal information the bank discloses and the categories of those third parties with whom the bank has contracted and state whether the third party is:
 - A service provider that performs marketing services on the bank's behalf or on behalf of the bank and another financial institution, or

- A financial institution with whom the bank has a joint marketing agreement.
- An explanation of the **right of the consumer to opt out** of the disclosure and the methods by which the consumer can exercise that right.
- Any disclosures the bank makes **under certain parts of the Fair Credit Reporting Act** (that is, notices regarding the ability to opt out of disclosures of information among affiliates).
- If the **bank discloses nonpublic personal information to third parties which are subject to an exception**, the bank is not required to list those exceptions in the initial or annual privacy notices. When describing the categories with respect to those parties, it is sufficient to state that the bank makes disclosures to other nonaffiliated companies:
 - For everyday business purposes, such as [include all that apply] to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus; or
 - As permitted by law; and
 - Any other information that the bank wishes to provide that applies to the bank and to the consumers to whom the privacy notice is being sent.

Regulatory Text

- (a) **General rule.** The initial, annual, and revised privacy notices that you provide under §§1016.4, 1016.5, and 1016.8 of this part must include each of the following items of information, in addition to any other information you wish to provide, that applies to you and to the consumers to whom you send your privacy notice:
- (1) The categories of nonpublic personal information that you collect;
 - (2) The categories of nonpublic personal information that you disclose;
 - (3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§1016.14 and 1016.15 of this part;
 - (4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§1016.14 and 1016.15;
 - (5) If you disclose nonpublic personal information to a nonaffiliated third party under §1016.13 (and no other exception in §1016.14 or §1016.15 applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;
 - (6) An explanation of the consumer's right under §1016.10(a) of this part to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

- (7) Any disclosures that you make under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);
 - (8) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
 - (9) Any disclosure that you make under paragraph (b) of this section.
- (b) **Description of nonaffiliated third parties subject to exceptions.** If you disclose nonpublic personal information to third parties as authorized under §§1016.14 and 1016.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§1016.4 and 1016.5. When describing the categories with respect to those parties, it is sufficient to state that you make disclosures to other nonaffiliated companies:
- (1) For your everyday business purposes, such as [*include all that apply*] to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus; or
 - (2) As permitted by law.
- (c) **Examples**
- (1) **Categories of nonpublic personal information that you collect.** You satisfy the requirement to categorize the nonpublic personal information that you collect if you list the following categories, as applicable:
 - (i) Information from the consumer;
 - (ii) Information about the consumer's transactions with you or your affiliates;
 - (iii) Information about the consumer's transactions with nonaffiliated third parties; and
 - (iv) Information from a consumer reporting agency.
 - (2) **Categories of nonpublic personal information you disclose.**
 - (i) You satisfy the requirement to categorize the nonpublic personal information that you disclose if you list the categories described in paragraph (c)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.
 - (ii) If you reserve the right to disclose all of the nonpublic personal information about consumers that you collect, you may simply state that fact without describing the categories or examples of the nonpublic personal information you disclose.
 - (3) **Categories of affiliates and nonaffiliated third parties to whom you disclose.** You satisfy the requirement to categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information if you list the following categories, as applicable, and a few examples to illustrate the types of third parties in each category.
 - (i) Financial service providers, followed by illustrative examples such as mortgage bankers, securities broker-dealers, and insurance agents;
 - (ii) Non-financial companies, followed by illustrative examples such as retailers, magazine publishers, airlines, and direct marketers; and

- (iii) Others, followed by examples such as nonprofit organizations.
- (4) **Disclosures under exception for service providers and joint marketers.** If you disclose nonpublic personal information under the exception in §1016.13 of this part to a nonaffiliated third party to market products or services that you offer alone or jointly with another financial institution, you satisfy the disclosure requirement of paragraph (a)(5) of this section if you:
- (i) List the categories of nonpublic personal information you disclose, using the same categories and examples you used to meet the requirements of paragraph (a)(2) of this section, as applicable; and
 - (ii) State whether the third party is:
 - (A) A service provider that performs marketing services on your behalf or on behalf of you and another financial institution; or
 - (B) A financial institution with whom you have a joint marketing agreement.

A Simplified Notice [12 C.F.R. § 1016.6(c)(5)]

Regulatory Discussion

The regulation provides for a simplified disclosure notice for a bank that does not disclose, and does not wish to reserve the right to disclose, nonpublic personal information to affiliates or nonaffiliated third parties except as authorized in the exceptions. In this case, the bank may simply state that fact and provide the following information, as described above:

- The categories of nonpublic personal information that the bank collects;
- The bank's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
- If the bank discloses nonpublic personal information to third parties which is subject to an exception, the bank is not required to list those exceptions in the initial or annual privacy notices. When describing the categories with respect to those parties, it is sufficient to state that the bank makes disclosures to other nonaffiliated companies:
 - For everyday business purposes, such as [include all that apply] to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus; or
 - As permitted by law.

Regulatory Text

- (5) **Simplified notices.** If you do not disclose, and do 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 §§1016.14 and 1016.15, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

Confidentiality and Security [12 C.F.R. § 1016.6(c)(6)]

Regulatory Discussion

The notice must describe in general terms how the bank protects the non-public personal information that it acquires.

- The **bank's policies and practices** with respect to protecting the confidentiality and security of nonpublic personal information. The bank fulfills this requirement if it does both of the following:
 - Describes in general terms who is authorized to have access to the information; and
 - 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.

Regulatory Text

- (6) **Confidentiality and security.** You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if you do both of the following:
- (i) Describe in general terms who is authorized to have access to the information; and
 - (ii) State whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use.

Short-Form initial Notice with Opt Out Notice for Non-Customers [12 C.F.R. § 1016.6(d)]

Regulatory Discussion

It is unlikely that this notice will be used by most banks, but the regulation does permit a shorter form for any privacy notices given to non-customers.

Regulatory Text

(d) Short-form initial notice with opt out notice for non-customers.

- (1) You may satisfy the initial notice requirements in §§1016.4(a)(2), 1016.7(b), and 1016.7(c) of this part for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in §1016.7.
- (2) A short-form initial notice must:
 - (i) Be clear and conspicuous;

- (ii) State that your privacy notice is available upon request; and
 - (iii) Explain a reasonable means by which the consumer may obtain that notice.
- (3) You must deliver your short-form initial notice according to §1016.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to §1016.9.
- (4) **Examples of obtaining privacy notice.** You provide a reasonable means by which a consumer may obtain a copy of your privacy notice if you:
- (i) Provide a toll-free telephone number that the consumer may call to request the notice; or
 - (ii) For a consumer who conducts business in person at your office, maintain copies of the notice on hand that you provide to the consumer immediately upon request.

Future Disclosures (optional) [12 C.F.R. § 1016.6(e)]

Regulatory Discussion

Optional text about future disclosures can be added.

The bank's notice may include the following:

- **Categories of nonpublic personal information the bank reserves the right to disclose** in the future, but does not currently disclose; and
- **Categories of affiliates or nonaffiliated third parties to whom the bank reserves the right to disclose** in the future, but to whom it does not currently disclose.

Regulatory Text

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

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

Model Privacy Notice [12 C.F.R. § 1016.6(f)]

Regulatory Discussion

Use of the model privacy notice constitutes compliance with this section.

Regulatory Text

(f) **Model privacy form.** Pursuant to §1016.2(a) of this part, a model privacy form that meets the notice content requirements of this section is included in the appendix to this part.

Section 8: Opt-Out Requirements

[12 C.F.R. § 1016.7]

Form of Opt-Out Notice [12 C.F.R. § 1016.7(a)]

Regulatory Discussion

General Information

If the bank intends to share outside of the exceptions [see Section 7], the bank must provide a “clear and conspicuous” [see formal definition, Section 2] opt-out notice to each of its consumers. The notice must state:

- That the bank discloses or reserves the right to disclose nonpublic personal information to a nonaffiliated third party;
- That the consumer has the right to opt out of that disclosure; and
- A reasonable means by which the consumer may exercise the opt-out right.

Note: While the first bullet point above expressly refers to disclosure of nonpublic personal information to a nonaffiliated third party, the revised Model form is designed to also satisfy an opt out of affiliate sharing.

Adequate Opt-Out Notices

The bank provides an adequate opt-out notice if it:

- Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose;
- Identifies all of the categories of nonaffiliated third parties to which the bank discloses the information;
- States that the consumer can opt out of the disclosure of that information; and
- 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.

Opt-Out Means

The bank provides a reasonable means to exercise an opt-out right if it:

- Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;
- Includes a reply form together with the opt-out notice which includes the bank’s mailing address;

- Provides an electronic means to opt out, such as a form that can be sent via e-mail or a process at the bank's Web site, if the consumer agrees to the electronic delivery of information; or
- Provides a toll-free telephone number that consumers may call to opt out.

The bank does not provide a reasonable means of opting out if the only way is:

- For the consumer to write his or her own letter; or
- By the use of a check-off box that was provided in the initial notice but not provided with any subsequent notice.

Examples of Reasonable Opportunity to Opt Out

- **By mail.** The bank mails the required notices 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 notices were mailed.
- **By electronic means.** A customer opens an online account with the bank and agrees to receive the required notices electronically. The bank allows the customer to opt out by any reasonable means within 30 days after the date the customer acknowledges receipt of the notices.

Miscellaneous Provisions

- The bank may require each consumer to opt out through a specific means, as long as it is reasonable for that consumer.

Regulatory Text

(a)

(1) **Form of opt out notice.** If you are required to provide an opt out notice under §1016.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. The notice must state:

- (i) That you disclose or reserve the right to disclose nonpublic personal information about your consumer to a nonaffiliated third party;
- (ii) That the consumer has the right to opt out of that disclosure; and
- (iii) A reasonable means by which the consumer may exercise the opt out right.

(2) **Examples**

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

- (A) Identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose, and all of the categories of nonaffiliated third parties to which you disclose the information, as described in §1016.6(a)(2) and (3) of this

part, and state that the consumer can opt out of the disclosure of that information;
and

- (B) Identify the financial products or services that the consumer obtains from you, either singly or jointly, to which the opt out direction would apply.
- (ii) **Reasonable opt out means.** You provide a reasonable means to exercise an opt out right if you:
- (A) Designate check-off boxes in a prominent position on the relevant forms with the opt out notice;
- (B) Include a reply form together with the opt out notice that, in the case of financial institutions described in §1016.3(l)(3) of this part, includes the address to which the form should be mailed;
- (C) Provide an electronic means to opt out, such as a form that can be sent via electronic mail or a process at your Web site, if the consumer agrees to the electronic delivery of information; or
- (D) Provide a toll-free telephone number that consumers may call to opt out.
- (iii) **Unreasonable opt out means.** You *do not* provide a reasonable means of opting out if:
- (A) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or
- (B) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that you provided with the initial notice but did not include with the subsequent notice.
- (iv) **Specific opt out means.** You may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

Notice Provisions [12 C.F.R. § 1016.7(b) and (c)]

Regulatory Discussion

- The bank may provide the opt-out notice with or on the same written or electronic form as the initial notice.
- If the bank provides the opt-out notice later than required for the initial notice, the bank must include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

Regulatory Text

- (b) **Same form as initial notice permitted.** You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with §1016.4.
- (c) **Initial notice required when opt out notice delivered subsequent to initial notice.** If you provide the opt out notice later than required for the initial notice in accordance with §1016.4 of this part, you must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

Joint Relationships [12 C.F.R. § 1016.7(d)]

Regulatory Discussion

If two or more consumers jointly obtain a financial product or service from the bank, a single opt-out notice may be provided. The opt-out notice must explain how the bank will treat an opt-out direction by a joint consumer.

- Any of the joint consumers may exercise the right to opt out. The bank may either:
 - Treat an opt-out direction by a joint consumer as applying to all of the joint consumers, or
 - Permit each joint consumer to opt out separately and allow one of the joint consumers to opt out on behalf of all of the joint consumers.
- The bank may not require all joint consumers to opt out before it implements any opt-out direction.

For example, if John and Mary have a joint checking account with a bank and arrange 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:

- Send a single opt-out notice to John's address, but the bank must accept an opt-out direction from either John or Mary.
- 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.
- Permit John and Mary to make different opt-out directions. If the bank does so:
 - It must permit John and Mary to opt out for each other;
 - If both opt out, the bank must permit both of them to notify the bank in a single response (such as on a form or through a telephone call); and
 - 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.

Regulatory Text

(d) **Joint relationships in the case of financial institutions other than credit unions and covered entities subject to FTC enforcement jurisdiction.** For purposes of this paragraph (d), “you” is limited to financial institutions other than credit unions and financial institutions described in §1016.3(l)(3) of this part.

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

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

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

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

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

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

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

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

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

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

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

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

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

Omitted Sections [12 C.F.R. § 1016.7(e) and (f)]

(e) **Joint relationships in the case of credit unions.** [Omitted].

(f) **Joint relationships in the case of covered entities subject to FTC enforcement jurisdiction.** [Omitted]

Complying with an Opt Out [12 C.F.R. § 1016.7(g) through (i)]

Regulatory Discussion

The bank must comply with the following opt-out rules:

- Comply with a consumer's opt-out direction as soon as reasonably practicable after the bank receives it.
- A consumer may exercise the right to opt out at any time.
- A consumer's direction to opt out is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Regulatory Text

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

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

(i) **Duration of consumer's opt out direction.**

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

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

Delivery [12 C.F.R. § 1016.7(j)]

Regulatory Discussion

Delivery must follow the standards set forth later in the regulation.

Regulatory Text

(j) **Delivery.** When you are required to deliver an opt out notice by this section, you must deliver it according to §1016.9 of this part.

Delivery [12 C.F.R. § 1016.7(k)]

Regulatory Discussion

Use of the model privacy notice constitutes compliance with this regulation.

Regulatory Text

(k) **Model privacy form.** Pursuant to §1016.2(a) of this part, a model privacy form that meets the notice content requirements of this section is included in the appendix to this part.

Section 9: Notice to Customers: Revised Privacy Notice [12 C.F.R. § 1016.8]

General Rule [12 C.F.R. § 1016.8(a)]

Regulatory Discussion

The bank must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice unless the bank has:

- Provided a clear and conspicuous revised notice that accurately describes its policies and practices;
- Provided a new opt-out notice;
- Given the consumer a reasonable opportunity to opt out; and
- The consumer does not opt out.

Regulatory Text

(a) **General rule.** Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to that consumer under §1016.4 of this part, unless:

- (1) You have provided to the consumer a clear and conspicuous revised notice that accurately describes your policies and practices;
- (2) You have provided to the consumer a new opt out notice;
- (3) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and
- (4) The consumer does not opt out.

Timing of the Revised Privacy Notice [12 C.F.R. § 1016.8(b)]

Regulatory Discussion

Except as otherwise permitted by the exceptions, the bank must provide a revised notice before it:

- Discloses a new category of nonpublic personal information to any nonaffiliated third party;

- Discloses nonpublic personal information to a new category of nonaffiliated third party; or
- Discloses 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.

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.

Regulatory Text

(b) Examples.

- (1) Except as otherwise permitted by §§1016.13, 1016.14, and 1016.15 of this part, you must provide a revised notice before you:
 - (i) Disclose a new category of nonpublic personal information to any nonaffiliated third party;
 - (ii) Disclose nonpublic personal information to a new category of nonaffiliated third party;
or
 - (iii) Disclose nonpublic personal information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.
- (2) A revised notice is not required if you disclose nonpublic personal information to a new nonaffiliated third party that you adequately described in your prior notice.

Delivery of the Revised Privacy Notice [12 C.F.R. § 1016.8(c)]

Regulatory Discussion

These notices must be delivered in writing or electronically (if the consumer agrees) so that each consumer can reasonably be expected to receive the actual notice.

Regulatory Text

- (c) **Delivery.** When you are required to deliver a revised privacy notice by this section, you must deliver it according to §1016.9 of this part.

Section 10: Delivery of Notices [12 C.F.R. § 1016.9]

Provision of Notices [12 C.F.R. § 1016.9(a) through (d)]

Regulatory Discussion

All notices must be delivered so that each consumer can reasonably be expected to receive the actual notice:

- In writing; or
- Electronically (if the consumer agrees).

Examples of Reasonable Expectation of Actual Notice Include:

- Hand-delivering a printed copy;
- Mailing a printed copy to the last known address of the consumer;
- Posting the notice on an electronic site and requiring the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service; or
- Posting the notice on the ATM screen and requiring the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

Examples of Unreasonable Expectations of Actual Notice Include:

- Only posting a sign in the bank's branch or office or generally publishing advertisements of the bank's privacy policies and practices; or
- Sending the notice via electronic mail to a consumer who does not obtain a financial product or service from the bank electronically.

Annual Notices Only

You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:

- The customer is a regular user of your website and agrees to receive notices at the website, or
- The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.

Oral Description of Notice Insufficient

The bank may not solely provide the notice by oral explanation, either in person or over the telephone.

Regulatory Text

- (a) **How to provide notices.** You 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.** You may reasonably expect that a consumer will receive actual notice if you:
- (i) Hand-deliver a printed copy of the notice to the consumer;
 - (ii) Mail a printed copy of the notice to the last known address of the consumer;
 - (iii) For the consumer who conducts transactions electronically:
 - (A) In the case of financial institutions other than those described in §1016.3(l)(3) of this part, post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service; or
 - (B) In the case of financial institutions described in §1016.3(l)(3), clearly and conspicuously post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service;
 - (iv) For an isolated transaction with the consumer, such as an ATM transaction, post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.
- (2) **Examples of unreasonable expectation of actual notice.** You may *not*, however, reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:
- (i) Only post a sign in your branch or office or generally publish advertisements of your privacy policies and practices; or
 - (ii) Send the notice via electronic mail to a consumer who does not obtain a financial product or service from you electronically.
- (c) **Annual notices only.** You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:
- (1) The customer uses your website to access financial products and services electronically and agrees to receive notices at the website, and you post your current privacy notice continuously in a clear and conspicuous manner on the website; or
 - (2) The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.
- (d) **Oral description of notice insufficient.** You may not provide any notice required by this part solely by orally explaining the notice, either in person or over the telephone.

Retention or Accessibility of Notices for Customers [12 C.F.R. § 1016.9(e)]

Regulatory Discussion

For customers only, the bank must provide the notice so that the customer can retain it or obtain it later in writing or, if the customer agrees, electronically. Examples of retention or accessibility include:

- Hand-delivering a printed copy of the notice to the customer;
- Mailing a printed copy of the notice to the last known address of the customer; or
- Making the 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.

Regulatory Text

(e) Retention or accessibility of notices for customers.

- (1) For customers only, you must provide the initial notice required by §1016.4(a)(1), the annual notice required by §1016.5(a), and the revised notice required by §1016.8 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.
- (2) **Examples of retention or accessibility.** You provide a privacy notice to the customer so that the customer can retain it or obtain it later if you:
 - (i) Hand-deliver a printed copy of the notice to the customer;
 - (ii) Mail a printed copy of the notice to the last known address of the customer, or, in the case of credit unions, mail a printed copy of the notice to the last known address of the customer upon request of the customer; or
 - (iii) Make your current privacy notice available on a Web site (or a link to another Web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the Web site.

Joint Notice with Other Financial Institutions [12 C.F.R. § 1016.9(f) through (h)]

Regulatory Discussion

The bank may provide a joint notice from the bank 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.

Regulatory Text

- (f) **Joint notice with other financial institutions.** You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions.
- (g) **Joint relationships in the case of financial institutions other than credit unions and covered entities subject to FTC enforcement jurisdiction.** For purposes of this paragraph (g), “you” is limited to financial institutions other than credit unions and the financial institutions described in §1016.3(l)(3). If two or more consumers jointly obtain a financial product or service from you, you may satisfy the initial, annual, and revised notice requirements of §§1016.4(a), 1016.5(a), and 1016.8(a), respectively, by providing one notice to those consumers jointly.
- (h) **Joint relationships in the case of covered entities subject to FTC enforcement jurisdiction.** [Omitted]
 - (i) **Joint relationships in the case of credit unions.** [Omitted]
 - (2) **Special rule for loans in the case of credit unions.** [Omitted]

Section 11: Limits on Disclosures

[12 C.F.R. § 1016.10]

Limitations on Disclosure of Nonpublic Information to Nonaffiliated Third Parties [12 C.F.R. § 1016.10(a)]

Regulatory Discussion

Unless otherwise authorized under specific exceptions, the bank may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:

- The bank has provided an initial notice to the consumer;
- The bank has provided an opt-out notice to the consumer;
- The bank has given the consumer a reasonable opportunity to opt out of the disclosure; and
- The consumer does not opt out.

The regulation becomes very repetitive regarding the definition of “opt-out” and the methods to do so.

Regulatory Text

(a)

- (1) **Conditions for disclosure.** Except as otherwise authorized in this part, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:
 - (i) You have provided to the consumer an initial notice as required under §1016.4 of this part;
 - (ii) You have provided to the consumer an opt out notice as required in §1016.7 of this part;
 - (iii) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and
 - (iv) The consumer does not opt out.
- (2) **Opt out definition.** Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§1016.13, 1016.14, and 1016.15.
- (3) **Examples of reasonable opportunity to opt out.** You provide a consumer with a reasonable opportunity to opt out if:

- (i) **By mail.** You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days from the date you mailed the notices.
- (ii) **By electronic means.** A customer opens an online account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.
- (iii) **Isolated transaction with consumer.** For an isolated transaction, such as the purchase of a cashier's check by a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

Scope of Opt Out [12 C.F.R. § 1016.10(b)]

Regulatory Discussion

The opt out applies regardless of whether a consumer has established a customer relationship with the bank. Additionally, the bank must comply with the opt-out disclosure requirements and cannot, directly or through any affiliate, disclose any nonpublic personal information about a consumer that the bank has collected, regardless of whether it collected the information before or after receiving the consumer's direction to opt out.

Regulatory Text

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

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

Partial Opt Out [12 C.F.R. § 1016.10(c)]

Regulatory Discussion

The bank may allow the consumer to opt out of certain nonpublic personal information or certain nonaffiliated third party sharing. Note: The use of this option would obviously present significant

recordkeeping challenges to the bank, keeping track on a consumer-by-consumer basis of what information and/or what third parties are subject to an opt out.

Regulatory Text

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

Section 12: Limits on Redisclosure and Reuse

[12 C.F.R. § 1016.11]

Limits on Redisclosure and Reuse of Information

Throughout this section of the manual, reference is made to “exceptions.” This portion of the regulation covers two situations:

- Information the bank receives from a nonaffiliated financial institution; and
- Limits on re-disclosure and reuse of information which others receive from the bank.

Information the Bank Receives Under an Exception [12 C.F.R. § 1016.11(a)]

Regulatory Discussion

If the bank receives nonpublic personal information from a nonaffiliated financial institution under an exception, the bank’s disclosure and use of that information is limited as follows:

- The bank may disclose the information to the affiliates of the financial institution from which the bank received the information;
- The bank may disclose the information to its affiliates, but the affiliates may, in turn, disclose and use the information only to the extent that the bank may disclose and use the information; and
- The bank may disclose and use the information pursuant to an exception in the ordinary course of business to carry out the activity covered by the exception under which the bank received the information.

For example if a bank receives a customer list from a nonaffiliated financial institution in order to provide account processing services under an exception, the bank may disclose that information under any exception 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.

Regulatory Text

(a)

- (1) **Information you receive under an exception.** If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in §1016.14 or

§1016.15 of this part, your disclosure and use of that information is limited as follows:

- (i) You may disclose the information to the affiliates of the financial institution from which you received the information;
 - (ii) You may disclose the information to your affiliates, but your affiliates may, in turn, disclose and use the information only to the extent that you may disclose and use the information; and
 - (iii) You may disclose and use the information pursuant to an exception in §1016.14 or §1016.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.
- (2) **Example.** If you receive a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in §1016.14(a), you may disclose that information under any exception in §1016.14 or §1016.15 in the ordinary course of business in order to provide those services. For example, you could disclose the information in response to a properly authorized subpoena or, in the case of financial institutions other than those described in §1016.3(l)(3), to your attorneys, accountants, and auditors. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

Information the Bank Receives Outside of an Exception [12 C.F.R. § 1016.11(b)]

Regulatory Discussion

If the bank receives nonpublic personal information from a nonaffiliated financial institution other than under an exception, the bank may disclose the information only to the following:

- Affiliates of the financial institution from which the bank received the information;
- To the bank's affiliates, but the affiliates may, in turn, disclose the information only to the extent that the bank can disclose the information; and
- 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.

For example, if the bank obtains a customer list from a nonaffiliated financial institution outside of the exceptions, it may do the following:

- The bank may use the list for its own purposes; and
- 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, such as to the bank's attorneys or accountants.

Regulatory Text

(b)

(1) **Information you receive outside of an exception.** If you receive nonpublic personal information from a nonaffiliated financial institution other than under an exception in §1016.14 or §1016.15 of this part, you may disclose the information only:

- (i) To the affiliates of the financial institution from which you received the information;
- (ii) To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and
- (iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.

(2) **Example.** If you obtain a customer list from a nonaffiliated financial institution outside of the exceptions in §§1016.14 and 1016.15:

- (i) You may use that list for your own purposes; and
- (ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed the list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list, as limited by the opt out direction of each consumer whose nonpublic personal information you intend to disclose, and you may disclose the list in accordance with an exception in §1016.14 or §1016.15, such as to your attorneys or accountants.

Information the Bank Discloses Under an Exception [12 C.F.R. § 1016.11(c)]

Regulatory Discussion

If the bank discloses nonpublic personal information to a nonaffiliated third party under an exception, the third party may disclose and use that information only as follows:

- To the bank's affiliates;
- 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
- The third party may disclose and use the information pursuant to an exception in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

Regulatory Text

(c) **Information you disclose under an exception.** If you disclose nonpublic personal

information to a nonaffiliated third party under an exception in §1016.14 or §1016.15 of this part, the third party may disclose and use that information only as follows:

- (1) The third party may disclose the information to your affiliates;
- (2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and
- (3) The third party may disclose and use the information pursuant to an exception in §1016.14 or §1016.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

Information the Bank Discloses Outside of an Exception [12 C.F.R. § 1016.11(d)]

Regulatory Discussion

If the bank discloses nonpublic personal information to a nonaffiliated third-party other than under an exception, the third-party may disclose the information only to the following:

- To the bank's affiliates;
- 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
- To any other person, if the disclosure would be lawful if the bank made it directly to that person.

Regulatory Text

(d) **Information you disclose outside of an exception.** If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in §1016.14 or §1016.15 of this part, the third party may disclose the information only:

- (1) To your affiliates;
- (2) To its affiliates, but its affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and
- (3) To any other person, if the disclosure would be lawful if you made it directly to that person.

Section 13: Limits on Sharing Account Number Information for Marketing Purposes

[12 C.F.R. § 1016.12]

General Prohibition on Disclosure of Account Numbers [12 C.F.R. § 1016.12(a)]

Regulatory Discussion

The bank may 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.

Regulatory Text

- (a) **General prohibition on disclosure of account numbers.** You must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a consumer's credit card account, deposit account, share 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.

Exceptions [12 C.F.R. § 1016.12(b)]

Regulatory Discussion

This general rule does not apply if the bank discloses an account number or similar form of access number or access code to either of the following:

- 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
- 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.

Regulatory Text

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

- (1) To your agent or service provider solely in order to perform marketing for your own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account; or
- (2) To a participant in a private label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

Examples [12 C.F.R. § 1016.12(c)]

Regulatory Discussion

- Account number
- Transaction account

Regulatory Text

(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 you do 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, a share account, or a credit card account. A transaction account does not include an account to which third parties cannot initiate charges.

Section 14: Exceptions [12 C.F.R. § 1016.13]

Exceptions to the Opt-Out Requirements for Service Providers and Joint Marketing [12 C.F.R. § 1016.13(a)]

Regulatory Discussion

The opt-out requirements 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:

- Provides the initial notice to the consumer; and
- 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 listed below in the ordinary course of business.

For example, if the 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 stated above 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 listed below in the ordinary course of business to carry out that joint marketing.

Regulatory Text

(a) General rule.

- (1) The opt out requirements in §§1016.7 and 1016.10 of this part do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf, if you:
 - (i) Provide the initial notice in accordance with §1016.4; and
 - (ii) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in §1016.14 or §1016.15 in the ordinary course of business to carry out those purposes.
- (2) **Example.** If you disclose nonpublic personal information under this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in §1016.14 or §1016.15 in the ordinary course of business to carry out that joint marketing.

Service May Include Joint Marketing [12 C.F.R. § 1016.13(b)]

Regulatory Discussion

The services a nonaffiliated third party performs for a bank under 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.

Regulatory Text

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

Definition of Joint Agreement [12 C.F.R. § 1016.13(c)]

Regulatory Text

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

Section 15: Exceptions [12 C.F.R. § 1016.14]

Exceptions to Notice and Opt-Out Requirements for Processing and Servicing Transactions [12 C.F.R. § 1016.14(a)]

Regulatory Discussion

The requirements for initial notice, opt out, and for service providers and joint marketing 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 the following:

- Servicing or processing a financial product or service requested or authorized by the consumer;
- Maintaining or servicing the consumer's account with the bank, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or
- A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer.

Regulatory Text

(a) **Exceptions for processing transactions at consumer's request.** The requirements for initial notice in §1016.4(a)(2), for the opt out in §§1016.7 and 1016.10, and for service providers and joint marketing in §1016.13 do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

- (1) Servicing or processing a financial product or service that a consumer requests or authorizes;
- (2) Maintaining or servicing the consumer's account with you, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or
- (3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

Underlying Definition [12 C.F.R. § 1016.14(b)]

Regulatory Discussion

The term “necessary to effect, administer, or enforce a transaction” means that the disclosure is:

- 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
- Required, or is a usual, appropriate, or acceptable method:
 - 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;
 - To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;
 - 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;
 - To accrue or recognize incentives or bonuses associated with the transaction that are provided by the bank or any other party;
 - To underwrite insurance at the consumer's request, for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or state law; or
 - In connection with:
 - 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;
 - The transfer of receivables, accounts, or interests therein; or
 - The audit of debit, credit, or other payment information.

Regulatory Text

- (b) **Necessary to effect, administer, or enforce a transaction** means that the disclosure is:
- (1) Required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or
 - (2) Required, or is a usual, appropriate or acceptable method:
 - (i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the consumer's account in the ordinary course of providing the financial service or financial product;

- (ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;
- (iii) To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;
- (iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;
- (v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or state law; or
- (vi) In connection with:
 - (A) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means;
 - (B) The transfer of receivables, accounts, or interests therein; or
 - (C) The audit of debit, credit, or other payment information.

Section 16: Exceptions [12 C.F.R. § 1016.15]

Other Exceptions to Notice and Opt-Out Requirements [12 C.F.R. § 1016.15]

Regulatory Discussion

The requirements for the initial notice, opt out, and for service providers and joint marketing do not apply when the bank discloses nonpublic personal information in the following circumstances:

- With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction. For example:
- 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.

A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic information.

- For the following protective or legal reasons:
 - To protect the confidentiality or security of the bank's records pertaining to the consumer, service, product, or transaction;
 - To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
 - For required institutional risk control or for resolving consumer disputes or inquiries;
 - To persons holding a legal or beneficial interest relating to the consumer; or
 - To persons acting in a fiduciary or representative capacity on behalf of the consumer.
- To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating the bank, persons that are assessing the bank's compliance with industry standards, and the bank's attorneys, accountants, and auditors.
- 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 USC 3401), to law enforcement agencies (including government regulators), self-regulatory organizations, or for an investigation on a matter related to public safety.
- To a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 USC1681) or from a consumer report reported by a consumer reporting agency.
- 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 that business or unit.

- To comply with Federal, state, or local laws, rules, and other applicable legal requirements, specifically:
 - To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities; or
 - To respond to judicial process or government regulatory authorities having jurisdiction over the bank for examination, compliance, or other purposes as authorized by law.

Regulatory Text

(a) **Exceptions to opt out requirements.** The requirements for initial notice in §1016.4(a)(2), for the opt out in §§1016.7 and 1016.10, and for service providers and joint marketing in §1016.13 do not apply when you disclose nonpublic personal information:

- (1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;
- (2)
 - (i) To protect the confidentiality or security of your records pertaining to the consumer, service, product, or transaction;
 - (ii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
 - (iii) For required institutional risk control or for resolving consumer disputes or inquiries;
 - (iv) To persons holding a legal or beneficial interest relating to the consumer; or
 - (v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;
- (3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants, and auditors;
- (4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*) to law enforcement agencies (including the Bureau, a Federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, with respect to any person domiciled in that insurance authority's state that is engaged in providing insurance, and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;
- (5)
 - (i) To a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*); or
 - (ii) From a consumer report reported by a consumer reporting agency;

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

(7)

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

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

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

(b) Examples of consent and revocation of consent.

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

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under §1016.7(h) of this part.

Section 17: Relation to Other Laws

[12 C.F.R. § 1016.16] and [12 C.F.R. § 1016.17]

Protection of Fair Credit Reporting Act [12 C.F.R. § 1016.16]

Regulatory Discussion

Nothing in this regulation shall be construed to modify, limit, or supersede the Fair Credit Reporting Act.

Regulatory Text

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.

Relation to State Laws [12 C.F.R. § 1016.17]

Regulatory Discussion

This regulation 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.

A state statute, regulation, order, or interpretation is not inconsistent with the provisions of this regulation if the protection such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this regulation, as determined by the Consumer Financial Protection Bureau (CFPB), after consultation with the bank's Federal regulatory agency, on the CFPB's own motion, or upon the petition of any interested party.

Regulatory Text

- (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 Bureau, on its own motion or upon the petition of any interested party, after consultation with the agency or authority with jurisdiction under section 505(a) of the GLB Act (15 U.S.C. 6805(a)) over either the person that initiated the complaint or that is the subject of the complaint.

Section 18: The Model Privacy Forms – Appendix A

| FACTS WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION? | | |
|---|--|--|
| Why? | Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do. | |
| What? | The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none"> ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] | |
| How? | All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing. | |
| | Reasons we can share your personal information | Does [name of financial institution] share? |
| | For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus | |
| | For our marketing purposes— to offer our products and services to you | |
| | For joint marketing with other financial companies | |
| | For our affiliates' everyday business purposes— information about your transactions and experiences | |
| | For our affiliates' everyday business purposes— information about your creditworthiness | |
| | For our affiliates to market to you | |
| | For nonaffiliates to market to you | |
| To limit our sharing | <ul style="list-style-type: none"> ■ Call [phone number]—our menu will prompt you through your choice(s) ■ Visit us online: [website] or ■ Mail the form below <p>Please note:</p> <p>If you are a <i>new</i> customer, we can begin sharing your information [30] days from the date we sent this notice. When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.</p> <p>However, you can contact us at any time to limit our sharing.</p> | |
| Questions? | Call [phone number] or go to [website] | |



| Mail-in Form | | |
|---|--|---------------------------------|
| <p>Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.]</p> <p><input type="checkbox"/> Apply my choices only to me]</p> | <p>Mark any/all you want to limit:</p> <p><input type="checkbox"/> Do not share information about my creditworthiness with your affiliates for their everyday business purposes.</p> <p><input type="checkbox"/> Do not allow your affiliates to use my personal information to market to me.</p> <p><input type="checkbox"/> Do not share my personal information with nonaffiliates to market their products and services to me.</p> | |
| | Name | Mail to: |
| | Address | [Name of Financial Institution] |
| | City, State, Zip | [Address1] |
| | [Account #] | [Address2] |
| | | [City], [ST] [ZIP] |

| Who we are | |
|--|---|
| Who is providing this notice? | [insert] |
| What we do | |
| How does [name of financial institution] protect my personal information? | To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert] |
| How does [name of financial institution] collect my personal information? | We collect your personal information, for example, when you <ul style="list-style-type: none"> ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.] |
| Why can't I limit all sharing? | Federal law gives you the right to limit only <ul style="list-style-type: none"> ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.] |
| What happens when I limit sharing for an account I hold jointly with someone else? | [Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account—unless you tell us otherwise.] |
| Definitions | |
| Affiliates | Companies related by common ownership or control. They can be financial and nonfinancial companies. <ul style="list-style-type: none"> ■ [affiliate information] |
| Nonaffiliates | Companies not related by common ownership or control. They can be financial and nonfinancial companies. <ul style="list-style-type: none"> ■ [nonaffiliate information] |
| Joint marketing | A formal agreement between nonaffiliated financial companies that together market financial products or services to you. <ul style="list-style-type: none"> ■ [joint marketing information] |
| Other important information | |
| [insert other important information] | |

Section 19: The Model Privacy Forms – Appendix B

B. General Instructions

1. How the Model Privacy Form Is Used

- (a) The model form may be used, at the option of a financial institution, including a group of financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in §§1016.6 and 1016.7 of this part.
- (b) The model form is a standardized form, including page layout, content, format, style, pagination, and shading. Institutions seeking to obtain the safe harbor through use of the model form may modify it only as described in these Instructions.
- (c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act [15 U.S.C. 1681-1681x] (FCRA), such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.
- (d) The word “customer” may be replaced by the word “member” whenever it appears in the model form, as appropriate.

2. The Contents of the Model Privacy Form

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

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

- (1) Date last revised (upper right-hand corner).
- (2) Title.
- (3) Key frame (Why?, What?, How?).
- (4) Disclosure table (“Reasons we can share your personal information”).
- (5) “To limit our sharing” box, as needed, for the financial institution's opt-out information.
- (6) “Questions” box, for customer service contact information.
- (7) Mail-in opt-out form, as needed.

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

- (1) Heading (Page 2).
- (2) Frequently Asked Questions (“Who we are” and “What we do”).
- (3) Definitions.
- (4) “Other important information” box, as needed.

3. The Format of the Model Privacy Form

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

- (a) **Easily readable type font.** Financial institutions that use the model form must use an easily readable type font. While a number of factors together produce easily readable type font, institutions are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between the lines of type.
- (b) **Logo.** A financial institution may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the model form or the space constraints of each page.
- (c) **Page size and orientation.** Each page of the model form must be printed on paper in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.
- (d) **Color.** The model form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the model form. Logos may also be printed in color.
- (e) **Languages.** The model form may be translated into languages other than English.

Section 20: The Model Privacy Forms – Appendix C

Introduction

This section includes the model form and the form’s instructions. The following discussion on how to complete the form considers each portion of the form, as applicable to the institution. Following some of the individual portions of the form, we have included Young & Associates, Inc. comments, which appear in text boxes. These comments relate to the applicability of that portion of the form given a bank’s particular circumstances. Other than our comments in the text boxes, all of the language in the balance of this section is a direct quote of the instructions. We have chosen the Opt-Out Version of the form, as it covers all areas more completely. As a result, some fields may not be applicable to your institution.

Revision Date / Title

Rev. [insert date]

FACTS

WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO
WITH YOUR PERSONAL INFORMATION?

Last Revised Date (Rev. [Insert Date])

The financial institution must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as “rev. [month/year]” using either the name or number of the month, such as “rev. March 2012” or “rev. 3/12”

Y&A Commentary – We have routinely recommended to client institutions to document revision dates on various disclosures, brochures, etc. This information makes it easy for institutions to quickly identify the latest version without a “text for text” comparison. As stated above, the model privacy form requires a revision date.

Institution’s Name [Name of Financial Institution]

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

Key Frame

Why?

| | |
|-------------|--|
| Why? | Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do. |
|-------------|--|

Describes the purpose of the privacy notice. There are no entries required for this part.

What?

| | |
|--------------|--|
| What? | <p>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none"> ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] <p>When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.</p> |
|--------------|--|

The bulleted list identifies the types of personal information that the institution collects and shares. All institutions must use the term “Social Security number” in the first bullet.

Institutions must use five (5) of the following terms to complete the bulleted list. The sample form has preset five of these as a guide, but they may be overwritten with the five selected by the institution as it relates to the information it collects and shares in its privacy practices.

- income;
- account balances;
- payment history;
- transaction history;
- transaction or loss history;
- credit history;
- credit scores;
- assets;
- investment experience;
- credit-based insurance scores;
- insurance claim history;

- medical information;
- overdraft history;
- purchase history;
- account transactions;
- risk tolerance;
- medical-related debts;
- credit card or other debt;
- mortgage rates and payments;
- retirement assets;
- checking account information;
- employment information;
- wire transfer instructions.

Y&A Commentary – As noted in the Instructions, institutions shall identify and disclose five of the items included in the list above as it relates to the types of information the institution collects and shares. Prior to creating your privacy form, you will need to determine which of above-mentioned items best belong in your list of five. Note that social security number is hard coded into the form and must be used.

How?

| | |
|-------------|---|
| How? | All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing. |
|-------------|---|

As noted in the general instructions above, financial institutions may substitute the term “customer” with the term “member” if appropriate.

The name of the financial institution will again appear in the “How?” box.

Disclosure Table (“Reasons we can share your personal information”)

The left column (below) lists reasons for sharing or using personal information. Each reason

correlates to a specific legal provision described in this Instruction.

In the middle column, each institution must provide a “Yes” or “No” response that accurately reflects its information sharing policies and practices with respect to the reason listed on the left.

In the right column, each institution must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

- “Yes” if it is required to or voluntarily provides an opt out;
- “No” if it does not provide an opt out; or
- “We don’t share” if it answers “No” in the middle column.

Only the sixth row (“For our affiliates to market to you”) may be omitted at the option of the institution. See paragraph C.2(d)(6) of this Instruction.

Specific Disclosures and Corresponding Legal Provisions

The following is a complete representation of this portion of the form. To simplify the step-by-step review, we have then reproduced each question for ease of illustration through the discussion of this section.

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

For our everyday business purposes

| | | |
|--|--|--|
| <p>For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus</p> | | |
|--|--|--|

This reason incorporates sharing information under §§ 1016.14 and 1016.15 and with service providers pursuant to § 1016.13 of this part other than the purposes “For our marketing purposes” or “For joint marketing with other financial companies” specified below in these Instructions.

Y&A Commentary – For most institutions, the answers to middle and right columns will be “Yes,” and “No,” respectively. This is because this type of sharing is permitted without an opt out and routinely used to effectuate transactions.

For our marketing purposes

| | | |
|--|--|--|
| <p>For our marketing purposes— to offer our products and services to you</p> | | |
|--|--|--|

This reason incorporates sharing information with service providers by an institution for its own marketing pursuant to § 1016.13 of this part. An institution that shares for this reason may choose to provide an opt out.

Y&A Commentary – For institutions that share customer information with service providers to market the institution’s products / services, the regulation does not require an opt out as long as the institution discloses this type of sharing and has entered into a contractual relationship with the third party. Therefore, the answers to middle and right columns will be “Yes” and “No,” respectively. However, at the institution’s option, it could offer an opt out for this type of sharing. In that case, the answer to the right column would then be “Yes.”

For institutions that do not share customer information with service providers, the answers to middle and right columns will be “No,” and “We don’t share,” respectively.

For joint marketing with other financial companies

| | | |
|--|--|--|
| For joint marketing with other financial companies | | |
|--|--|--|

This reason incorporates sharing information under joint marketing agreements between two or more financial institutions and with any service provider used in connection with such agreements pursuant to § 1016.13 of this part. An institution that shares for this reason may choose to provide an opt out.

Y&A Commentary – Essentially, the answers / guidance to the “marketing purpose” question above apply in the “joint marketing” as well, as follows:

For institutions that share customer information under a joint marketing relationship, the regulation does not require an opt out as long as the institution discloses this type of sharing and has entered into a contractual relationship with the third-party. Therefore, the answers to middle and right columns will be “Yes” and “No,” respectively. However, at the institution’s option, it could offer an opt out for this type of sharing. In that case, the answer to the right column would then be “Yes.”

For institutions that do not share customer information with service providers, the answers to middle and right columns will be “No,” and “We don’t share,” respectively.

For our affiliates’ everyday business purposes—information about transactions and experiences

| | | |
|--|--|--|
| For our affiliates’ everyday business purposes— information about your transactions and experiences | | |
|--|--|--|

This reason incorporates sharing information specified in sections 603(d)(2)(A)(i) and (ii) of the FCRA. An institution that shares for this reason may choose to provide an opt-out.

Y&A Commentary – This question is directed to whether the institution shares information about a customer’s transactions or experiences with the institution’s affiliate(s).

For institutions that have affiliates and do share transaction or experience information with the affiliates, then the answers to the middle and right columns would be “Yes” and “No,” respectively, if the institution chooses not to provide an opt out. This type of sharing is governed by the Fair Credit Reporting Act (FCRA) under the definition of an exclusion to a “consumer report” as defined in the FCRA. Specifically, the following is one of the consumer report exclusions: “a report containing information solely as to transactions or experiences between the consumer and the person making the report and communication of that information among persons related by common ownership or affiliated by corporate control.”

However, if the institution chooses to provide an opt out for this type of sharing, the answers for the middle and right columns would each be “Yes.”

Institutions that do not share with affiliates would answer by entering in “No” and “We don’t share” in both columns.

For our affiliates’ everyday business purposes—information about creditworthiness.

| | | |
|--|--|--|
| For our affiliates’ everyday business purposes— information about your creditworthiness | | |
|--|--|--|

This reason incorporates sharing information pursuant to section 603(d)(2)(A)(iii) of the FCRA. An institution that shares for this reason must provide an opt out.

Within the preamble to the final rule, the Agencies also provided guidance for institutions choosing to include or exclude the affiliate marketing notice and related opt out within the privacy form. Specifically, they state the following:

“Including the affiliate marketing notice and opt out in the model form is optional. Institutions that are required to provide this notice, and elect not to include it in their GLB Act privacy notice, must separately send an affiliate marketing notice that complies fully with the affiliate marketing rule requirements.

For those institutions that elect to incorporate this provision in the model form, the Agencies believe that it is simpler and less confusing to consumers for the affiliate marketing opt out to be of indefinite duration, consistent with the opt out required under the GLB Act.

If an institution elects to limit the time period for which the opt out is effective, as permitted under the affiliate marketing rule, it must not include the affiliate marketing opt out in the model form. Instead, the institution must comply separately with the specific affiliate marketing rule requirements.”

Y&A Commentary – This question is directed to whether the institution shares information about a customer’s creditworthiness with the institution’s affiliate(s).

For institutions that have affiliates and do share customer creditworthiness information with the affiliates, then the answers to the middle and right columns would each be “Yes.” This type of sharing is governed by the Fair Credit Reporting Act (FCRA) under the definition of an exclusion to a “consumer report” as defined in the FCRA. Specifically, the following is the consumer report exclusions: “communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons.”

Institutions that do not share with affiliates would answer by entering in “No” and “We don’t share” in both columns.

For our affiliates to market to you

| | | |
|--|--|--|
| For our affiliates to market to you | | |
|--|--|--|

This reason incorporates sharing information specified in section 624 of the FCRA. This reason may be omitted from the disclosure table when:

- the institution does not have affiliates (or does not disclose personal information to its affiliates);
- the institution’s affiliates do not use personal information in a manner that requires an opt out; or the institution provides the affiliate marketing notice separately.

Institutions that include this reason must provide an opt out of indefinite duration. An institution that is required to provide an affiliate marketing opt out, but does not include that opt out in the model form under this part, must comply with the implementing regulations with respect to the initial notice and opt out and any subsequent renewal notice and opt out. An institution not required to provide an opt out under this subparagraph may elect to include this reason in the model form.

Y&A Commentary – As noted in the instructions, this question may be omitted from the privacy form if the institution does not share with affiliates that will market to the institution’s customers.

However, if the institution does have one or more affiliates to whom it will share customer information (regardless of the type of information) and the affiliate(s) may market its products or services to that customer, then this question must remain. To answer such scenarios, the answers to the middle and right columns would each be “Yes.”

For nonaffiliates to market to you

| | | |
|---|--|--|
| For nonaffiliates to market to you | | |
|---|--|--|

This reason incorporates sharing described in §§ 1016.7 and 1016.10(a) of this part. An institution that shares personal information for this reason must provide an opt out.

Y&A Commentary – Institutions that do share with nonaffiliates with the intention that such entities will market to the institution’s customers, must provide an opt-out.

Therefore, if the institution does share customer information with a nonaffiliate and the nonaffiliate may market its products or services to that customer, then the answers to the middle and right columns would each be “Yes.”

For institutions that do not share outside of the exceptions, the answer for the middle and right columns would be “No” and “We don’t share,” respectively.

To Limit Our Sharing

| | |
|-----------------------------|--|
| <p>To limit our sharing</p> | <ul style="list-style-type: none"> ■ Call [phone number]—our menu will prompt you through your choice(s) ■ Visit us online: [website] or ■ Mail the form below <p>Please note:</p> <p>If you are a <i>new</i> customer, we can begin sharing your information [30] days from the date we sent this notice. When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.</p> <p>However, you can contact us at any time to limit our sharing.</p> |
|-----------------------------|--|

A financial institution must include this section of the model form only if it provides an opt out. Specifically, institutions using the model form must include the opt-out section in their notices only if they:

- share or use information in a manner that triggers an opt out, or
- choose to provide opt outs beyond what is required by law.

Financial institutions that provide opt outs are not required to provide all the opt-out choices and methods described in the model form; they should select those that accurately reflect their practices.

Institutions must select one or more of the applicable opt-out methods described:

- telephone, such as by a toll-free number;
- a Web site; or
- use of a mail-in opt-out form.

Institutions may include the words “toll-free” before telephone, as appropriate. In addition, the word “choice” may be written in either the singular or plural, as appropriate.

An institution that allows consumers to opt out online must provide either a specific Web address that takes consumers directly to the opt-out page or a general Web address that provides a clear and conspicuous direct link to the opt-out page.

The opt-out choices made available to the consumer who contacts the institution through these methods must correspond accurately to the “Yes” responses in the third column of the disclosure table. In the part titled “Please note,” institutions may insert a number that is 30 or greater in the space marked “[30].” Instructions on voluntary or state privacy law opt-out information are located elsewhere in these Instructions.

Y&A Commentary – For institutions voluntarily or required to provide an opt-out, the privacy form must include this section of the model form. The model version appearing here in this manual is “Version 3” from the final rule and allows for the three types of opt-out methods (i.e., phone, online and mail-in). If your institution chooses not to allow the “mail-in” option, you will want to use Version 2, which only allows opt out by phone or online. Regardless, the institution allowing an opt out must state the number of days a customer has to opt out, which may not be less than 30.

Institutions not voluntarily or required to provide an opt out would use Version 1. This version does not include the “To limit our sharing” portion.

Questions Box

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

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

Mail-in Form (Part of Version 3)

✂

| Mail-in Form | | | | | | | | | | |
|--|--|------|--|---------|--|------------------|--|-------------|--|---|
| <p>Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.]</p> <p><input type="checkbox"/> Apply my choices only to me]</p> | <p>Mark any/all you want to limit:</p> <p><input type="checkbox"/> Do not share information about my creditworthiness with your affiliates for their everyday business purposes.</p> <p><input type="checkbox"/> Do not allow your affiliates to use my personal information to market to me.</p> <p><input type="checkbox"/> Do not share my personal information with nonaffiliates to market their products and services to me.</p> | | | | | | | | | |
| | <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #cccccc;">Name</td> <td style="width: 50%;"></td> </tr> <tr> <td style="background-color: #cccccc;">Address</td> <td></td> </tr> <tr> <td style="background-color: #cccccc;">City, State, Zip</td> <td></td> </tr> <tr> <td style="background-color: #cccccc;">[Account #]</td> <td></td> </tr> </table> | Name | | Address | | City, State, Zip | | [Account #] | | <p>Mail to:</p> <p>[Name of Financial Institution] [Address1] [Address2] [City], [ST] [ZIP]</p> |
| Name | | | | | | | | | | |
| Address | | | | | | | | | | |
| City, State, Zip | | | | | | | | | | |
| [Account #] | | | | | | | | | | |

Financial institutions must include this mail-in form only if they state in the “To limit our sharing” box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the “Yes” responses in the third column in the disclosure table.

Institutions that require customers to provide only name and address may omit the section identified as “[account #].” Institutions that require additional or different information, such as a random opt-out number or a truncated account number, to implement an opt-out election should modify the “[account #]” reference accordingly. This includes institutions that require customers with multiple accounts to identify each account to which the opt out should apply. An institution must enter its opt-out mailing address: in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the model form.

Joint Accountholder

Only institutions that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with these Instructions, must include in the far left column of the mail-in form the following statement:

“If you have a joint account, your choice (s) will apply to everyone on your account unless you mark below. Apply my choice(s) only to me.”

The word “choice” may be written in either the singular or plural, as appropriate. Financial institutions that provide insurance products or services, provide this option, and elect to use the model form may substitute the word “policy” for “account” in this statement. Institutions that do not provide this option may eliminate this left column from the mail-in form.

FCRA Section 603(d)(2)(A)(iii) opt out

If the institution shares personal information pursuant to section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

“Do not share information about my creditworthiness with your affiliates for their everyday business purposes.”

FCRA Section 624 opt out

If the institution incorporates section 624 of the FCRA in accordance with these Instructions, it must include in the mail-in opt-out form the following statement:

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

Nonaffiliate Opt out

If the financial institution shares personal information pursuant to § 1016.10(a) of this part, it must include in the mail-in opt-out form the following statement:

“Do not share my personal information with nonaffiliates to market their products and services to me.”

Additional Opt Outs

Financial institutions that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt outs in this section of the model form. A financial institution that chooses to offer an opt out for its own marketing in the mail-in opt-out form must include one of the two following statements:

“Do not share my personal information to market to me; or

Do not use my personal information to market to me.”

A financial institution that chooses to offer an opt out for joint marketing must include the following statement:

“Do not share my personal information with other financial institutions to jointly market to me.”

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

Frequently Asked Question - Who we are?

| | |
|-------------------------------|----------|
| Page 2 | |
| Who we are | |
| Who is providing this notice? | [insert] |

This question may be omitted where only one financial institution provides the model form and that institution is clearly identified in the title on page one. Two or more financial institutions that jointly provide the model form must use this question to identify themselves as required by § 1016.9(f) of this part. Where the list of institutions exceeds four (4) lines, the institution must describe in the response to this question the general types of institutions jointly providing the notice and must separately identify those institutions, in minimum 8-point font, directly following the “Other important information” box, or, if that box is not included in the institution’s form, directly following the “Definitions.” The list may appear in a multi-column format.

Frequently Asked Questions - What we do?

The following represents the portion of the form that contains the questions on what the institution does with regards to customer information. We have included the entire portion of this part of the form below for contextual purpose and then examine each question individually.

| What we do | |
|--|---|
| How does [name of financial institution] protect my personal information? | To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert] |
| How does [name of financial institution] collect my personal information? | We collect your personal information, for example, when you <ul style="list-style-type: none"> ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.] |
| Why can't I limit all sharing? | Federal law gives you the right to limit only <ul style="list-style-type: none"> ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.] |
| What happens when I limit sharing for an account I hold jointly with someone else? | [Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account—unless you tell us otherwise.] |

How does the institution protect personal information?

| What we do | |
|--|---|
| How does [name of financial institution] protect my personal information? | To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert] |

The financial institution may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the institution's use of cookies or other measures it uses to safeguard personal information. Institutions are limited to a maximum of 30 additional words.

How does the institution collect personal information?

| | |
|--|---|
| <p>How does [name of financial institution] collect my personal information?</p> | <p>We collect your personal information, for example, when you</p> <ul style="list-style-type: none"> ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] <p>[We also collect your personal information from other companies.]</p> <p>OR</p> <p>[We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]</p> |
|--|---|

Institutions must use five (5) of the following terms to complete the bulleted list for this question:

- open an account;
- deposit money;
- pay your bills;
- apply for a loan;
- use your credit or debit card;
- seek financial or tax advice;
- apply for insurance;
- pay insurance premiums;
- file an insurance claim;
- seek advice about your investments;
- buy securities from us;
- sell securities to us;
- direct us to buy securities;
- direct us to sell your securities;
- make deposits or withdrawals from your account;
- enter into an investment advisory contract;
- give us your income information;
- provide employment information;
- give us your employment history;
- tell us about your investment or retirement portfolio;
- tell us about your investment or retirement earnings;
- apply for financing;
- apply for a lease;
- provide account information;

- give us your contact information;
- pay us by check;
- give us your wage statements;
- provide your mortgage information;
- make a wire transfer;
- tell us who receives the money;
- tell us where to send the money;
- show your government-issued ID;
- show your driver’s license;
- order a commodity futures or option trade.

Y&A Commentary – As noted in the Instructions, institutions shall identify and disclose five of the items included in the list above as it relates to how the institution collects customer information. Prior to creating your privacy form, you will need to determine which of above-mentioned items best belong in your list of five.

Institutions that collect personal information from their affiliates and/or credit bureaus must include after the bulleted list the following statement:

“We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.”

Institutions that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead:

“We also collect your personal information from other companies.”

Only institutions that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

Why can’t consumer limit all sharing?

| | |
|--|---|
| <p>Why can't I limit all sharing?</p> | <p>Federal law gives you the right to limit only</p> <ul style="list-style-type: none"> ■ sharing for affiliates’ everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you <p>State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]</p> |
|--|---|

Institutions that describe state privacy law provisions in the “Other important information” box must use the bracketed sentence:

“See below for more on your rights under state law.”

Other institutions must omit this sentence.

What happens when consumer limits sharing of joint account?

| | |
|---|--|
| <p>What happens when I limit sharing for an account I hold jointly with someone else?</p> | <p>[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account—unless you tell us otherwise.]</p> |
|---|--|

Only financial institutions that provide opt-out options must use this question. Other institutions must omit this question. Institutions must choose one of the following two statements to respond to this question:

“Your choices will apply to everyone on your account.”

or

“Your choices will apply to everyone on your account—unless you tell us otherwise.”

Financial institutions that provide insurance products or services and elect to use the model form may substitute the word “policy” for “account” in these statements.

Definitions

| Definitions | |
|-------------------------------|---|
| <p>Affiliates</p> | <p>Companies related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"> ■ [affiliate information] |
| <p>Nonaffiliates</p> | <p>Companies not related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"> ■ [nonaffiliate information] |
| <p>Joint marketing</p> | <p>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.</p> <ul style="list-style-type: none"> ■ [joint marketing information] |

The financial institution must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

Affiliates. As required by § 1016.6(a)(3) of this part, where [affiliate information] appears, the financial institution must:

- If it has no affiliates, state:
 - “[name of financial institution]has no affiliates”;
- If it has affiliates but does not share personal information, state:
 - “[name of financial institution] does not share with our affiliates”; or
- If it shares with its affiliates, state, as applicable:
 - “Our affiliates include companies with a [common corporate identity of financial institution] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies;] and others, such as [insert illustrative list].”

Nonaffiliates. As required by § 1016.6(c)(3) of this part, where [nonaffiliate information] appears, the financial institution must:

- If it does not share with nonaffiliated third-parties, state:
 - “[name of financial institution]does not share with nonaffiliates so they can market to you”; or
- If it shares with nonaffiliated third-parties, state, as applicable:
 - “Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations].”

Joint Marketing. As required by § 1016.13 of this part, where [joint marketing] appears, the financial institution must:

- If it does not engage in joint marketing, state:
 - “[name of financial institution] doesn’t jointly market”; or
- If it shares personal information for joint marketing, state, as applicable:
 - “Our joint marketing partners include [list categories of companies such as credit card companies].”

“Other Important Information” box, as needed

| Other important information |
|--------------------------------------|
| [insert other important information] |

This box is optional. The space provided for information in this box is not limited. Only the following types of information can appear in this box.

- State and/or international privacy law information; and/or
- Acknowledgment of receipt form.

Online Form Builder

On April 15, 2010, the Federal functional regulators, including the FRB, FDIC, OCC and OTS announced the released of their “Model Consumer Privacy Notice Online Form Builder.” The following text is taken directly from the announcement:

“The Online Form Builder, based on the model form regulation published in the *Federal Register* on December 1, 2009, under the Gramm-Leach-Bliley Act, is available with several options. Easy-to-follow instructions for the form builder will guide an institution to select the version of the model form that fits its practices, such as whether the institution provides an opt out for consumers.

To obtain a legal “safe harbor” and so satisfy the law’s disclosure requirements, institutions must follow the instructions in the model form regulation when using the Online Form Builder.

The model privacy form was developed jointly by the Board of Governors of the Federal Reserve System, Commodity Futures Trading Commission, Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and Securities and Exchange Commission.

The Online Form Builder is available at:

http://www.federalreserve.gov/bankinfo/privacy_notice_instructions.pdf

The Agencies will post a link to this site on their websites.”

The following page is what you will see when accessing the link above.

Instructions for using the Privacy Notice Online Form Builder

1. Select your form, based on (1) whether you provide an opt out , (2) whether you include affiliate marketing, and (3) whether you use a mail-back form:

If you provide an opt out and you want to include affiliate marketing, use [Form 1](#).

If you provide an opt out and you do not want to include affiliate marketing, use [Form 2](#).

If you do not provide an opt out and you want to include affiliate marketing, use [Form 3](#).

If you do not provide an opt out and you do not want to include affiliate marketing, use [Form 4](#).

If you provide an opt out, you want to include affiliate marketing, and you have a mail-back form, use [Form 5](#).

If you provide an opt out, you do not want to include affiliate marketing, and you have a mail-back form, use [Form 6](#).

2. The PDF forms have fillable areas, indicated by the shaded boxes outlined in red. Place your cursor in the box and fill in the appropriate text.

The mail-back forms also include shaded boxes for optional text. These forms are designed to be printed on 8½ x 14 inch paper. To create the square for the opt-out provisions in the mail back form, use the square bracket and underline keys, followed by the text as provided in the rule. For example:

Do not share my personal information with nonaffiliates to market their products and services to me.

To learn more about the required text for each section, see the final rule notice published in the *Federal Register* on December 1, 2009 (pp. 62890–62994). The notice is available in PDF format at www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_FR.pdf or in HTML format at www.gpo.gov/fdsys/pkg/FR-2009-12-01/html/E9-27882.htm.

For institutions supervised by the following agencies, information required to fill in the forms is detailed beginning on the *Federal Register* page number specified below:

| <u>Supervising Agency</u> | <u>Page</u> |
|---|-------------|
| Office of the Comptroller of the Currency | 62916 |
| Federal Reserve System | 62925 |
| Federal Deposit Insurance Corporation | 62935 |
| Office of Thrift Supervision | 62945 |
| National Credit Union Administration | 62955 |
| Federal Trade Commission | 62965 |
| Commodity Futures Trading Commission | 62974 |
| Securities and Exchange Commission | 62984 |

3. If you have questions about the forms or any of the information required to fill in the designated areas, contact your federal regulator listed on p. 62890 of the *Federal Register* Notice.

4. If you have technical problems accessing these forms, please use the [Contact Us](#) link at the bottom of the page. Please provide a phone number where we can reach you.

http://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf

September 3, 2010

Sample Completed Form – No Opt Out / No Sharing

Rev. 01/2011

| FACTS | WHAT DOES National Bank of Anytown DO WITH YOUR PERSONAL INFORMATION? | | | | | | | | | | | | | | | | | | | | | | |
|--|--|-----------------------------|--|--------------------------------------|-----------------------------|--|-----|----|--|----|----------------|--|----|----------------|--|----|----------------|--|----|----------------|------------------------------------|----|----------------|
| Why? | Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do. | | | | | | | | | | | | | | | | | | | | | | |
| What? | <p>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none"> ■ Social Security number and income ■ account balances and payment history ■ credit history and credit scores <p>When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.</p> | | | | | | | | | | | | | | | | | | | | | | |
| How? | All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons National Bank of Anytown chooses to share; and whether you can limit this sharing. | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 45%;">Reasons we can share your personal information</th> <th style="width: 25%;">Does National Bank of Anytown share?</th> <th style="width: 30%;">Can you limit this sharing?</th> </tr> </thead> <tbody> <tr> <td>For our everyday business purposes—such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus</td> <td style="text-align: center;">Yes</td> <td style="text-align: center;">No</td> </tr> <tr> <td>For our marketing purposes—to offer our products and services to you</td> <td style="text-align: center;">No</td> <td style="text-align: center;">We don't share</td> </tr> <tr> <td>For joint marketing with other financial companies</td> <td style="text-align: center;">No</td> <td style="text-align: center;">We don't share</td> </tr> <tr> <td>For our affiliates' everyday business purposes—information about your transactions and experiences</td> <td style="text-align: center;">No</td> <td style="text-align: center;">We don't share</td> </tr> <tr> <td>For our affiliates' everyday business purposes—information about your creditworthiness</td> <td style="text-align: center;">No</td> <td style="text-align: center;">We don't share</td> </tr> <tr> <td>For nonaffiliates to market to you</td> <td style="text-align: center;">No</td> <td style="text-align: center;">We don't share</td> </tr> </tbody> </table> | | | Reasons we can share your personal information | Does National Bank of Anytown share? | Can you limit this sharing? | For our everyday business purposes—such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus | Yes | No | For our marketing purposes—to offer our products and services to you | No | We don't share | For joint marketing with other financial companies | No | We don't share | For our affiliates' everyday business purposes—information about your transactions and experiences | No | We don't share | For our affiliates' everyday business purposes—information about your creditworthiness | No | We don't share | For nonaffiliates to market to you | No | We don't share |
| Reasons we can share your personal information | Does National Bank of Anytown share? | Can you limit this sharing? | | | | | | | | | | | | | | | | | | | | | |
| For our everyday business purposes—such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus | Yes | No | | | | | | | | | | | | | | | | | | | | | |
| For our marketing purposes—to offer our products and services to you | No | We don't share | | | | | | | | | | | | | | | | | | | | | |
| For joint marketing with other financial companies | No | We don't share | | | | | | | | | | | | | | | | | | | | | |
| For our affiliates' everyday business purposes—information about your transactions and experiences | No | We don't share | | | | | | | | | | | | | | | | | | | | | |
| For our affiliates' everyday business purposes—information about your creditworthiness | No | We don't share | | | | | | | | | | | | | | | | | | | | | |
| For nonaffiliates to market to you | No | We don't share | | | | | | | | | | | | | | | | | | | | | |
| Questions? | Call 800-555-1212 or go to www.nationalbankofanytown.com | | | | | | | | | | | | | | | | | | | | | | |

| Who we are | |
|---|--|
| Who is providing this notice? | National Bank of Anytown |
| What we do | |
| How does National Bank of Anytown protect my personal information? | To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. |
| How does National Bank of Anytown collect my personal information? | <p>We collect your personal information, for example, when you</p> <ul style="list-style-type: none"> ■ open an account or deposit money ■ pay your bills or apply for a loan ■ use your credit or debit card <p>We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.</p> |
| Why can't I limit all sharing? | <p>Federal law gives you the right to limit only</p> <ul style="list-style-type: none"> ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you <p>State laws and individual companies may give you additional rights to limit sharing.</p> |
| Definitions | |
| Affiliates | <p>Companies related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"> ■ National Bank of Anytown has no affiliates. |
| Nonaffiliates | <p>Companies not related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"> ■ National Bank of Anytown does not share with nonaffiliates so they can market to you. |
| Joint marketing | <p>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.</p> <ul style="list-style-type: none"> ■ National Bank of Anytown doesn't jointly market. |
| Other important information | |
| | |