Regulation P: Privacy of Consumer Financial Information

Small-Entity Compliance Guide

Board of Governors of the Federal Reserve System
June 2002

CONTENTS

I. INTRODUCTION

The Board's Regulation P implements sections 502–509 of title V of the Gramm-Leach-Bliley Act--the portion of the act that concerns the privacy of consumer financial information.[1] Enacted on November 12, 1999, the Gramm-Leach-Bliley Act (GLB Act) was intended to enhance competition for financial products and services. Title V governs a financial institution's treatment of nonpublic personal information about consumers and requires that an institution, under certain circumstances, notify consumers about its privacy policies and practices. With certain exceptions, the act prohibits a financial institution from disclosing a consumer's nonpublic personal information to a nonaffiliated third party unless the institution satisfies various notice requirements and the consumer does not elect to prevent, or "opt out of," the disclosure. The act also imposes specific requirements regarding the disclosure of customer account numbers and the reuse and redisclosure of information a financial institution provides to a third party.

Purpose of the Guide

This Small-Entity Compliance Guide is intended to help financial institutions within the Board's primary jurisdiction comply with Regulation P, which is referred to hereinafter as the Privacy Rule.[2] Those institutions are

- State member banks
- Bank holding companies

[1]Regulation P is comparable to and consistent with the regulations issued by the other agencies that have responsibilities for implementing the Gramm-Leach-Bliley privacy provisions. The Board, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (collectively, the "banking agencies") jointly published privacy regulations for the financial institutions within their respective jurisdictions. *See* 65 Fed. Reg. 35,162 (June 1, 2000). The banking agencies developed their regulations in consultation with one another and with the National Credit Union Administration, the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC). The Commodity Futures Trading Commission, under the Commodity Exchange Act, 7 U.S.C. § 7b-2, as amended by the Commodity Futures Modernization Act of 2000, has also issued a privacy regulation that applies to entities within its jurisdiction.

[2] The Board's Privacy Rule is codified at 12 C.F.R. pt. 216. In this guide, citations of the rule omit the preceding title and publication references and refer only to the appropriate section number.

The guide is issued in accordance with the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857, *reprinted in* 5 U.S.C. § 601, note (West 1996).

- Subsidiaries or affiliates of state member banks and bank holding companies, except subsidiaries that are regulated by another functional regulator (such as national banks regulated by the OCC, state non-member banks regulated by the FDIC, registered securities broker-dealers and registered investment companies regulated by the SEC, and state-regulated insurance companies)
- Edge and agreement corporations
- Insured state agencies and state branches of foreign banks
- Commercial lending companies that are owned or controlled by foreign banks.

For simplicity, these entities are referred to throughout the guide as "you." The general term "financial institution" refers both to you and to any other institution that engages in an activity described in § 4(k) of the Bank Holding Company Act that is financial in nature or incidental thereto. 12 U.S.C. § 1843(k) (as amended by § 103 of the GLB Act).[3]

Scope of Privacy Rule and Guide; Relation of GLB Act to Other Laws

The Privacy Rule governs only your treatment of nonpublic personal information about your consumers. It does not apply to information about individuals or other entities that conduct transactions with you that you collect only for business purposes. And it does not apply to information that is not nonpublic personal information.

You must comply with each provision of the Privacy Rule that applies to your information-collection and information-disclosure practices. Although the guide is designed to help you identify and comply with all relevant requirements, it is not intended as a substitute for the provisions of the Privacy Rule. Acting in accordance with any particular section of the guide may not constitute compliance with all the requirements of the Privacy Rule that apply to you. In addition, the guide addresses only your obligations under the GLB Act and the Privacy

[3] Thus, a company traditionally associated with the provision of financial products and services, such as a securities broker-dealer or an insurance company, is a financial institution. In addition, a company normally associated with providing commercial products or services may be a financial institution for purposes of the GLB Act if its business also consists of financial activities, as defined in the privacy regulation adopted by the FTC. 16 C.F.R. 313.3(k)(1). Recognizing whether a company is a financial institution for purposes of title V of the GLB Act is an important aspect of complying with the limitations on redisclosing and reusing nonpublic personal information, as described in section VII.

Rule. It does not provide guidance for complying with provisions of federal or state law that could apply to your information practices, such as the Fair Credit Reporting Act.

Fair Credit Reporting Act

The GLB Act and the Privacy Rule do not modify, limit, or supersede the operation of the Fair Credit Reporting Act (FCRA), which governs the treatment of consumer reports and the obligations of consumer reporting agencies. When both the GLB Act and the FCRA apply to your disclosure of information about a consumer, you must comply with the requirements of both statutes. Compliance with the GLB Act and the Privacy Rule might not satisfy all your obligations under the FCRA.

State law

The Privacy Rule does not supersede, alter, or affect any state statute, regulation, order, or interpretation that is more protective of a consumer than the rule, as determined by the FTC.

II. IMPORTANT TERMS USED IN THE PRIVACY RULE

To understand the substantive requirements of the Privacy Rule, it is important first to understand the basic terms used throughout the rule, particularly the following:

Consumers and Customers

Consumers

A *consumer* is an individual who obtains or has obtained from you a financial product or service that is to be used primarily for personal, family, or household purposes and includes such an individual's legal representative. § 216.3(e). An individual who has not previously engaged in a transaction with you becomes your consumer when he or she obtains a financial product or service in an isolated transaction, such as by purchasing a money order from you. A consumer includes an individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she qualifies for a loan. A consumer also includes an individual who applies to you for a loan, regardless of whether you actually extend credit to that person. In addition, someone who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or economic advisory services from you is also a consumer, even if you do not establish an ongoing relationship with that individual.

Customers

A *customer* is a consumer with whom you have a "customer relationship." § 216.3(h). A customer relationship is a continuing relationship between you and a consumer 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. § 216.3(i). For example, you and a consumer establish a customer relationship when the consumer

- Opens and maintains a deposit or investment account with you
- Obtains a loan from you
- Enters into a lease of personal property with you
- Obtains financial, investment, or economic advisory services from you for a fee.

Special rule for loans

A special rule for loans governs a customer relationship that arises out of a loan transaction. § 216.4(c)(2). You establish a customer relationship with a consumer when you lend to him or her, even if you plan to assign the loan and (or) the servicing rights to another party shortly thereafter. After the loan is originated, the customer relationship follows the servicing rights to, rather than the ownership of, the loan. If you transfer to a third party the servicing rights of a loan you originated and have no other ongoing relationship with the borrower, he or she no longer is your customer even if you still own the loan. A borrower for whom you did not originate a loan becomes your customer when you acquire the servicing rights to his or her loan.

Categories of Information

The Privacy Rule identifies three categories of information--personally identifiable financial information, publicly available information, and nonpublic personal information. However, the rule protects only the third type. The definitions of the other types of information work together to define what constitutes nonpublic personal information.

Personally identifiable financial information

Personally identifiable financial information is any information you collect about a consumer in connection with providing a financial product or service to that consumer. § 216.3(o). This includes

- Information a consumer provides to you to obtain a financial product or service from you (for example, the consumer's name, phone number, address, and income)
- Information about a consumer resulting from any transaction involving a financial product or service between you and a consumer (for example, payment history, loan or deposit balances, and credit card purchases)
- Information that you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer (for example, information from a consumer report).

Personally identifiable financial information also includes the very fact that an individual is or has been your consumer as well as any information disclosed in a manner that indicates that the individual is or has been your consumer. *See* § 216.3(o)(2)(i)(C)-(D).

Publicly available information

Publicly available information is any information that you have a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records, widely distributed media, or disclosures to the general public that are required to be made by federal, state, or local law. § 216.3(p)(1). You have a "reasonable basis" to believe information is publicly available if you have taken steps to determine (1) that the information is of the type that is available to the general public and (2) whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not made such a direction. § 216.3(p)(2).

Any information that satisfies these two criteria is publicly available information, regardless of the source of that information. For instance, if your records contain a particular customer's phone number, you may consider that number to be publicly available if, for example, you determine that it is listed in a public directory. Similarly, certain mortgage documents or assessed property values are publicly available if you take steps to determine that such information is of the type that state or local law requires to be filed in the public record.

Nonpublic personal information

Nonpublic personal information, the category of information the Privacy Rule protects, consists of

- Personally identifiable financial information that is not publicly available information
- Lists, descriptions, or other groupings of consumers (including publicly available information contained therein) that are derived using personally identifiable financial information that is not publicly available. § 216.3(n).

When a list or other grouping of consumers is generated using customer relationships, loan balances, account numbers, or other personally identifiable financial information that is not publicly available, all information contained in that list--including any publicly available information about the consumers--is nonpublic personal information. By contrast, lists or other groupings of consumers that contain and are created using only publicly available information do not constitute nonpublic personal information. For example, in a political jurisdiction in which mortgage documents are public records, a list of the names and addresses contained in

those records of individuals who obtained a mortgage from you would not be nonpublic personal information if you used only publicly available information to create the list. All the information contained in the list would become nonpublic personal information, however, if the list contained or was created using nonpublic personal information, such as current loan balances.

Nonaffiliated Third Parties

The Privacy Rule generally restricts the disclosure of nonpublic personal information to nonaffiliated third parties. A *nonaffiliated third party* is any person except (1) your affiliate or (2) a person employed jointly by you and a company that is not your affiliate. § 216.3(m). Your "affiliate" is any company that controls, is controlled by, or is under common control with you. § 216.3(a). Your affiliates include your subsidiaries, your holding company, and any subsidiaries of your holding company.

III. DISCLOSURES TO NONAFFILIATED THIRD PARTIES

General Duty to Provide Privacy and Opt-Out Notices

The Privacy Rule requires you to notify your consumers about your policies and practices regarding the treatment of nonpublic personal information on various occasions. These privacy notice requirements are closely linked to the disclosures of nonpublic personal information you make (or reserve the right to make) and whether a consumer is entitled to opt out of those disclosures. This subsection gives an overview of the various types of notices required by the Privacy Rule. Following subsections discuss when you may disclose nonpublic personal information to nonaffiliated third parties. Requirements related to the content and delivery of notices are discussed in detail in section IV.

The first type of notice you must provide to a consumer is an "initial notice." You must provide an initial notice to a consumer not later than when he or she establishes a customer relationship with you, regardless of your disclosure practices. § 216.4(a)(1). In contrast, you owe an initial notice to a consumer who is not your customer only if (1) you plan to disclose nonpublic personal information about him or her to a nonaffiliated third party and (2) you are not allowed to make the disclosure(s) under an exception to the general notice and opt-out requirements (discussed later in this section). § 216.4(a)(2).

Regardless of whether a consumer is your customer, you must give the consumer an "opt-out" notice that both describes the consumer's right to opt out and provides instructions about how he or she can exercise that right before you disclose nonpublic personal information about the consumer, unless an exception applies. § 216.7.

For customers only, you must also provide an "annual notice" of your privacy policies and practices not less than annually during the continuation of the customer relationship. § 216.5.

Before disclosing nonpublic personal information about a consumer other than as described in the most recent privacy notice you provided to him or her, you must provide a "revised notice" that reflects these changes, a new opt-out notice, and another reasonable opportunity to opt out. § 216.8.

Disclosures Permitted Only if You Provide Notice and a Reasonable Opportunity to Opt Out

In general, you may not disclose nonpublic personal information about a consumer to any nonaffiliated third party unless

- You provide the consumer with an initial notice and an opt-out notice
- You provide the consumer a reasonable opportunity to opt out
- The consumer does not exercise his or her right to opt out. § 216.10(a)(1).

If all three conditions are met, you may disclose nonpublic personal information about the consumer in accordance with policies and practices described in your privacy notice.

The GLB Act and §§ 216.13, 216.14, and 216.15 of the Privacy Rule set forth various exceptions to this general rule. The exceptions allow you to disclose nonpublic personal information about the consumer without providing him or her with a privacy notice and (or) a reasonable opportunity to opt out, as explained more fully later in this section.[4]

Providing a reasonable opportunity to opt out

Whether you have given the consumer a reasonable opportunity to opt out depends on the facts and circumstances of the particular transaction and involves consideration of several factors, including how you provide your initial and opt-out notices, the means by which you give the consumer the opportunity to opt out, and the length of time you wait before determining that the consumer has not opted out. The Privacy Rule provides three examples of what constitutes a reasonable opportunity to opt out:

- If you deliver the initial and opt-out notices by mail, you provide a reasonable opportunity to opt out if you allow the consumer 30 days after you mail the notice to (1) return an opt-out form included in your mailing, (2) call a toll free number, or (3) communicate with you through other reasonable means that allow the consumer to make an opt-out election within 30 days.

[4] Disclosures made in reliance on an exception are referred to in this guide as disclosures made "under an exception." Those made in reliance on a consumer's decision not to opt out are referred to as disclosures made "outside an exception."

- If a customer opens an on-line account and agrees to receive the related privacy notices electronically, you provide a reasonable means of opting out by allowing the customer to opt out within 30 days after the date the customer acknowledges receipt of the notices in conjunction with opening the account.
- For an isolated transaction (for example, the purchase of a cashiers check), you provide a consumer a reasonable opportunity to opt out if you give the required notices at the time of the transaction and ask the consumer to make an opt-out decision before completing the transaction. § 216.10(a)(3).

You may require a consumer to opt out through a certain method, provided the method you require is reasonable for that particular consumer. You may not, however, require that a consumer write his or her own opt-out direction as the only means of exercising the opt-out right. § 216.7(a)(2)(iii). 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.

Complying with a consumer's decision to opt out

In general

A consumer may opt out at any time. § 216.7(f). If a consumer opts out within a reasonable period after receiving your opt-out notice, you may not disclose the consumer's nonpublic personal information unless the disclosure is permitted by an exception. § 216.10(a). If a consumer who did not opt out during the "reasonable period" later decides to opt out, you must stop disclosing his or her nonpublic personal information as soon as reasonably practicable after receiving the opt-out direction, unless the disclosure is permitted by an exception. § 216.7(e). Regardless of when a consumer opts out, you must comply with the opt-out direction until the consumer revokes that direction in writing (or, if the consumer has agreed, electronically). § 216.7(g).

Opt-out directions of former customers

If your customer opts out and the customer relationship is later terminated, you still may not disclose any nonpublic personal information you collected about that consumer during or related to the customer relationship unless the individual revokes his or her earlier opt-out direction. § 216.7(g)(2). If a former customer later establishes a new customer relationship with you, the opt-out direction that applied to the former relationship does not apply to the new relationship. Rather, you must give the individual new initial and opt-out notices and a reasonable opportunity to opt out of your disclosures of information associated with the new relationship.

Special considerations regarding joint relationships

When two or more consumers obtain a product or service from you jointly, each individual consumer associated with the joint transaction has, and may exercise, the right to opt out. However, you may elect to treat an opt-out direction by an individual consumer who is a party to a joint relationship in one of two ways. Your opt-out notice must explain your approach; that is, you must explain how you will treat an opt-out direction by an individual who is party to a joint relationship with you. § 216.7(d)(1).

Under one option, you may treat an opt-out direction by one consumer as applying to all the consumers associated with the jointly obtained product or service. § 216.7(d)(2)(i). In this case, if any consumer exercises his or her opt-out right, you must not disclose the nonpublic personal information of any of the associated consumers to a nonaffiliated third party except as permitted by an exception.

Under the other option, you may allow each consumer associated with the jointly obtained product or service to exercise his or her opt-out right on an individual basis. § 216.7(d)(2)(ii). In this case, the opt-out direction of one consumer applies only to your disclosure of that particular consumer's nonpublic personal information. You may not, however, require all the associated consumers to opt out before you implement the opt-out direction of any one of those consumers. If you allow consumers who jointly obtain a product or service from you to opt out separately, you must permit one consumer to opt out on behalf of all the associated consumers. § 216.7(d)(3).

Disclosures Permitted without Providing Notice and (or)

a Reasonable Opportunity to Opt Out

Sections 216.13, 216.14, and 216.15 of the Privacy Rule set forth the circumstances under which you are relieved of your general obligation to provide a consumer with notice and (or) an opportunity to opt out before disclosing nonpublic personal information to a nonaffiliated third party. Regardless of whether a consumer is your customer, you need not provide a consumer with an opportunity to opt out when you disclose the consumer's nonpublic personal information under any of the exceptions listed in §§ 216.13, 216.14, and 216.15. The exceptions at §§ 216.14 and 216.15 also allow you to disclose information about a consumer who is not your customer without providing an initial notice. You still must provide an initial notice to any consumer whose nonpublic personal information you disclose under § 216.13, and you must always provide an initial notice to your customer, regardless of which exception applies.

Exceptions for processing transactions, servicing accounts, and other purposes

Notice and opt-out exceptions described in § 216.14

The exceptions in § 216.14 generally permit you to disclose nonpublic personal information as needed to carry out routine activities in connection with a broad range of financial products and services without providing the consumer with notice and an opportunity to opt out. For example, you may disclose nonpublic personal information to a nonaffiliated third party in order to

- Process a financial product or service that a consumer requests or authorizes
- Service your mortgages
- Securitize your loans or sell them in the secondary market
- Prepare or mail your monthly account statements
- Make account information available to customers on your web site
- Underwrite title insurance at a customer's request
- Verify the sufficiency of funds in a customer's account
- Collect a check
- Collect a debt.

Notice and opt-out exceptions described in § 216.15

Section 216.15 provides additional exceptions that permit you to disclose nonpublic personal information to nonaffiliated third parties without providing a consumer with notice and an opportunity to opt out. For example, you may disclose nonpublic personal information in accordance with § 216.15 if a consumer consents to or directs the specific disclosure, such as when the consumer applies for a mortgage and specifically agrees that you may share that fact with a nonaffiliated insurance company that can offer the consumer homeowner's insurance. Section 216.15 also allows you to disclose nonpublic personal information to

- A person acting in a fiduciary or representative capacity on behalf of the consumer
- A person, such as a nonaffiliated software vendor, in order to protect the confidentiality or security of your consumer records
- Your auditors, attorneys, and accountants
- A consumer reporting agency
- A law enforcement agency in accordance with the Right to Financial Privacy Act.

In addition, you may disclose nonpublic personal information under § 216.15 to comply with a properly authorized subpoena or with federal, state, or local laws.

Opt-out exception for service providers and joint marketing agreements with financial institutions described in § 216.13

Section 216.13 allows you to disclose a consumer's nonpublic personal information to a nonaffiliated third party who performs services for you or functions on your behalf without providing the consumer an opt-out notice. However, to qualify for this exception, you must (1) enter into a contractual agreement prohibiting the third-party recipient from disclosing or using the nonpublic personal information other than to carry out the purpose(s) for which you disclose the information and (2) provide an initial notice to the consumer, whether or not he or she is your customer, that includes a separate statement describing the categories of information you disclose and the parties with whom you have contracted. §§ 216.6(a)(5) and 216.13(a)(1). If you satisfy these requirements, you could, for example, enter an arrangement under which you disclose nonpublic personal information to a nonaffiliated third party that markets your own financial products and services, such as a telemarketer or direct mail marketer.

Section 216.13 also allows you to provide nonpublic personal information to a nonaffiliated third party that markets financial products or services under an agreement

between you and another financial institution. § 216.13(b). To disclose information under such a marketing agreement without triggering a consumer's opt-out right, you must fulfill the two requirements described in the preceding paragraph and must have a joint agreement with the other financial institution under which the two of you jointly offer, endorse, or sponsor a financial product or service. § 216.13(c). The joint agreement must be a written contract, but the Privacy Rule does not impose any particular requirements as to the form, scope, duration, or other terms of that contract. § 216.13(c).

IV. WHEN AND HOW YOU MUST PROVIDE NOTICES

You must notify customers of your privacy policies and practices at various times.

Initial Notices

Notices to customers generally

You must provide an initial notice that accurately describes your privacy policies and practices to each of your customers, regardless of your disclosure practices. § 216.4(a)(1). For instance, you must provide an initial notice to a consumer who opens a credit card or checking account with you even if you share the account holder's nonpublic personal information only with nonaffiliated third parties under an exception.

New customers

With the exception of the two situations described in the following paragraph, you must provide an initial notice to a new customer not later than when you and the consumer establish a customer relationship. For instance, you must provide an initial notice to a consumer not later than when that consumer signs the contract to open a checking account, and you could provide the notice together with the account agreement and signature card. Similarly, if the customer relationship arises out of a loan transaction, you must provide an initial notice not later than when the consumer obtains credit, and you could provide the notice together with the documents or other forms that constitute the loan contract. You must always provide an initial notice when you originate a loan, even if you plan to transfer the loan and (or) the associated servicing rights shortly thereafter.

Section 216.4(e) allows you to deliver an initial privacy notice within a reasonable time *after* you establish a customer relationship under only two circumstances:

- If the consumer did not elect to establish the customer relationship (for example, if you acquire servicing rights to a consumer's loan and he or she had no choice about your acquisition of those rights)
- If providing the notice at the time you establish the relationship would substantially delay the customer's transaction (for example, if a consumer contracts for investment

advisory services by phone and wants to obtain your advice immediately) and the customer agrees to receive the notice at a later time.

If a customer relationship is initiated in person at your office or through other means by which the customer may view your notice, providing the notice at the time you establish the relationship will not substantially delay the customer's transaction. In such cases, you must deliver the notice not later than when you establish the relationship.

You may, of course, always deliver an initial privacy notice earlier than required.

Existing customers

When your existing customer obtains an additional financial product or service from you, you need not provide another initial notice to that customer if the earlier notice accurately describes your policies and practices regarding information you collect in connection with the subsequent product or service. § 216.4(d). For instance, if Joe Smith becomes your customer when he opens a checking account with you, you comply with the initial notice requirement if you provide an initial notice to Joe together with the deposit contract. If Joe maintains his checking account and obtains a loan from you six months later, you are not required to provide another initial notice to Joe if the previous notice you provided him also is accurate as to his new loan account.

Consumers who are not customers

You need not provide an initial notice to a consumer with whom you do not have a customer relationship unless (1) you plan to disclose nonpublic personal information about the consumer to a nonaffiliated third party and (2) no exception in § 216.14 or § 216.15 permits the disclosure. § 216.4(a)(2), (b). Suppose, for example, that an individual has no ongoing relationship with you but uses your ATM to withdraw funds from a checking account at another institution. This individual is your consumer, but even repeated use by the consumer of your ATM will not establish a customer relationship. You therefore owe this consumer an initial notice only if you plan to disclose his or her nonpublic personal information and no exception applies.

Opt-Out Notices

Regardless of whether a consumer is your customer, you must provide an opt-out notice before disclosing nonpublic personal information about the consumer to a nonaffiliated third party, unless an exception in § 216.13, 216.14, or 216.15 permits each disclosure you contemplate.

Annual Notices

In general

You must provide an annual notice to your customer as long as the customer relationship continues. § 216.5(a). You must give an annual notice at least once in any period of 12 consecutive months in which the customer relationship exists. You may define the 12-consecutive-month period that governs the timing of your annual notices, but you must apply that period to the customer consistently.

Non-customers

You need not provide annual notices to a consumer who is not your customer. For example, you have no obligation to provide annual notice to a consumer whose only transaction with you is using your ATM to withdraw funds from an account maintained at another bank, even if that consumer conducts transactions at your ATM over a period of years. You also need not provide an annual notice to a consumer who is your former customer. For example, if your customer relationship with Sally Smith is based only on her deposit account with you, the customer relationship terminates when Sally closes that account, and you need not continue providing annual notices to her. If Sally has more than one account with you, she remains your customer, and you must provide annual notice to her as long as she maintains at least one of her accounts with you. If Sally closes all her accounts with you and later opens a new account with you, she is entitled to a new initial notice at the time she opens the new account and annual notices thereafter while the account remains open.

Special rules for loan relationships

The special rule for loans discussed in section II affects when you owe an annual notice to a borrower. Because a customer relationship arising from a loan follows the servicing rights to the loan, you must provide an annual notice to a borrower for whose loan you have the servicing rights, even if you do not own the loan. You need not provide an annual notice to a borrower if you do not have servicing rights to his or her loan, even if you originated and (or) own the loan.

Revised Notices

The Privacy Rule is designed in part to enable your consumers to make opt-out decisions based on an accurate description of your privacy policies and practices. Generally, before disclosing nonpublic personal information about a consumer to a nonaffiliated third party other than as described in your most recent privacy notice, you must provide the consumer a revised initial notice, a new opt-out notice, and reasonable opportunity to opt out. You may make a new type of disclosure only if the consumer does not opt out in response to the revised notices. The duty to provide a revised notice could arise when you wish to disclose nonpublic personal information (1) that the categories of nonpublic personal information in your previous notice did not describe or (2) to a category of nonaffiliated third party that you did not previously identify as a recipient of such information.

You are not required to provide a revised notice when you make certain kinds of changes to your privacy policies or practices. For example, a revised notice is not required if you disclose nonpublic personal information to a particular new nonaffiliated third party that you adequately described in your prior notice. Regardless of whether you must provide a revised notice before making a new type of disclosure, your next annual notice to your customers must accurately describe your privacy policies and practices in effect at the time you send the notice.

The examples in the following sections help illustrate occasions when revised notice is and is not required.

Example of when revised notice is required

Suppose the most recent privacy notice you gave to Joe Smith states that you disclose nonpublic personal information only to nonaffiliated financial service providers. After providing this notice, you decide to disclose nonpublic personal information to a nonaffiliated airline, and no exception permits the disclosure. Because the airline does not fit within the category of recipients of nonpublic personal information you previously identified, you must provide Joe with a revised privacy notice, another opt-out notice, and a reasonable opportunity to opt out before disclosing his nonpublic personal information to the airline.

Example of when revised notice is not required

Suppose your most recent privacy notice to Joe Smith stated that you disclose, or may disclose, nonpublic personal information to your affiliates, financial service providers, nonfinancial companies, and others. When Joe did not opt out, you began disclosing nonpublic personal information about him to nonaffiliated insurance companies in accordance with your notice. Suppose you now wish to begin disclosing nonpublic personal information about Joe to a nonaffiliated securities firm and to a phone company. Your previous notice to Joe adequately described these new recipients because it stated that you might disclose information to financial services companies and nonfinancial companies. Thus, you do not owe Joe Smith a revised notice and need not provide him a new opportunity to opt out before disclosing his nonpublic personal information to the securities firm and phone company.

Delivery of Privacy Notices--Reasonable Expectation of Actual Notice

In general

You must deliver all privacy and opt-out notices so that each consumer to whom you owe the notice can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically. § 216.9(a).

You may satisfy the general requirement by either hand-delivering a printed copy of a privacy or opt-out notice to the consumer or mailing a copy of the notice to the consumer's last known address. For example, you could hand-deliver initial and opt-out notices to a consumer together with a deposit account agreement. If that consumer opens

a deposit account with you, you then could mail the required annual notice to his or her last known address. If a consumer conducts transactions electronically, you may also satisfy the general requirement if you post the required notice(s) on your web site and require the consumer to click through the pages that display the notice(s) as a necessary step to obtaining a particular financial product or service. § 216.9(b)(1)(iii). For an isolated transaction, such as an ATM transaction, you may post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice in order to withdraw funds. § 216.9(b)(1)(iv).

Special rules for delivery of annual notices only

If a customer uses your web site to access financial products and services (such as electronic bill payment) and agrees to receive notices at your web site, you may reasonably expect the customer to receive actual notice of your annual privacy notice if you continuously post your current privacy notice on the web site in a clear and conspicuous manner. If a customer has asked you to stop sending him or her information regarding the customer relationship, you may reasonably expect that customer to receive actual notice of your annual privacy notice if your current privacy notice is available to the customer upon request. § 216.9(c).

Additional requirements for customers only

You must provide all required initial, annual, and revised notices so that your customer can retain them or obtain them later in writing or, if the customer agrees, electronically. § 216.9(e). You satisfy this requirement if you hand-deliver the notice to the consumer or mail it to the consumer's last known address. If the customer has agreed to receive notices at your web site, you satisfy the requirement if you make your current privacy notice available on your web site or through a link to another web site.

Delivering notices regarding joint relationships

You may deliver one initial, annual, or revised privacy notice concerning a joint customer relationship to all the associated customers jointly. § 216.9(g). For example, if two consumers have a joint deposit account with you, you may send one notice to both account holders jointly at one account holder's address. Similarly, you may provide a single opt-out notice to two or more consumers who jointly obtain a product or service from you. § 216.7(d). As discussed in section III, each consumer has and may exercise the right to opt out, and your opt-out notice must explain your opt-out policies regarding joint relationships.

V. INFORMATION REQUIREMENTS FOR NOTICES

Requirements for Initial, Annual, and Revised Privacy Notices

In general

Although the required contents of your privacy notices depend on your specific disclosure practices, the Privacy Rule generally requires that you provide each of the following types of information

- The categories of nonpublic personal information you collect
- The categories of nonpublic personal information you disclose about your consumers and former customers
- The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your consumers and former customers, except those parties to whom you disclose information under §§ 216.14 and 216.15
- A statement describing your disclosure of nonpublic personal information under an exception listed in § 216.14 or § 216.15, if you make such disclosures (You are not required to list those exceptions in your initial and annual privacy notices or provide detailed information about the parties to whom you make such disclosures; rather, you are allowed to state only that you make disclosures to other nonaffiliated third parties as permitted by law. § 216.6(b))
- If you disclose nonpublic personal information under § 216.13 and no other exception in § 216.14 or § 216.15 permits the disclosure, a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted under § 216.13
- An explanation of the consumer's right to opt out of disclosures of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time
- Any notices you may provide under the FCRA regarding the ability to opt out of disclosures of information among affiliates
- Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Appendix A of the Privacy Rule provides sample clauses that illustrate some of the requirements concerning the content of notices. You may use an appropriate sample clause to satisfy one or more of the content requirements that apply to your information practices as long as the clause(s) you use accurately describe(s) your actual policies and practices. Because the information requirements are the same for each type of privacy notice, your initial and annual notices could in some cases be identical. You must, of course, incorporate any revisions you make to your privacy policies and practices into your annual notice.

Your notice may include items in addition to those the Privacy Rule requires. For example, your notice may list categories of nonpublic personal information you do not disclose currently but reserve the right to disclose. Similarly, your notice may list categories of nonaffiliated third parties to whom you do not currently disclose nonpublic personal information but to whom you reserve the right to disclose such information. Your notice also may include any other information you wish to provide.

Simplified notices

If you neither disclose nor reserve the right to disclose nonpublic personal information except to nonaffiliated third parties as permitted by the exceptions in §§ 216.14 and 216.15, your initial, annual, and revised privacy notices may simply state that fact. § 216.6(c)(5). This type of notice, called a "simplified notice," must also include an accurate description of the following items of information:

- The categories of nonpublic personal information you collect
- Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information
- The fact that you do not disclose nonpublic personal information about current and former customers to affiliates or nonaffiliated third parties, except as authorized by §§ 216.14 and 216.15. To satisfy this requirement, the notice may simply state that you make disclosures to nonaffiliated third parties as permitted by law.

Short-form initial notices

When you wish to disclose nonpublic personal information about a consumer who is not your customer outside the exceptions, you may choose to provide a short-form initial notice along with your opt-out notice. § 216.6(d). This situation could arise, for example, when a consumer uses your ATM or purchases travelers checks from you but conducts no other business with you. A short-form notice need state only that your complete privacy notice is available upon request and explain how the consumer can obtain it.

Requirements for Opt-Out Notices

Before disclosing outside an exception any nonpublic personal information about a consumer to a nonaffiliated third party, you first must give the consumer an opt-out notice stating

- That you disclose, or reserve the right to disclose, such information
- That the consumer has the right to opt out of the disclosure
- How the consumer may exercise the opt-out right. § 216.7(a)(1).

You are deemed to provide an adequate notice of the first two items above if you identify the categories of nonpublic personal information you may disclose and the categories of nonaffiliated third parties to which you disclose such information and state that the consumer may opt out of the disclosures. As discussed in section III, your opt-out notice must also describe how you will treat an opt-out direction by a consumer who obtains a product or service from you jointly with other consumers.

"Clear and Conspicuous" Standard

All privacy and opt-out notices must be clear and conspicuous, which means that the notice must be (1) reasonably understandable and (2) designed to call attention to the nature and significance of the information in the notice. § 216.3(b). You must present your notices in a manner that complies with this provision in each medium through which you provide notices. The Privacy Rule contains several examples that illustrate ways in which you can satisfy both elements of the "clear and conspicuous" standard using various media. § 216.3(b)(2).

VI. PROHIBITION AGAINST THE DISCLOSURE OF ACCOUNT NUMBERS

You generally must not disclose an account number or similar form of access number or access code to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. § 216.12. This prohibition applies even with respect to disclosures to a third party who markets financial products or services for you under a joint agreement in accordance with § 216.13. The prohibition does not, however, prevent you from disclosing an encrypted account number to a nonaffiliated third party, as long as you do not also disclose to that party the key to decrypt the number.

There are three exceptions to the general prohibition on account number disclosures. You may disclose an account number or other similar account access code to (1) a consumer reporting agency, (2) an agent or service provider who markets your own products or services, as long as the agent or service provider is not authorized to initiate charges directly to the account, and (3) participants in a private-label credit card program or an affinity or other similar program, as long as the participants in the program are identified to the customer when he or she enters the program.

VII. LIMITATIONS ON THE REDISCLOSURE AND REUSE OF INFORMATION

For purposes of this section, the term "recipient" refers to you when you receive nonpublic personal information from a nonaffiliated financial institution and to any nonaffiliated entity to which you give nonpublic personal information. A recipient is limited in its ability to redisclose and (or) use the nonpublic personal information it receives. The precise limits depend on (1) whether the recipient received the information under an exception listed at § 216.14 or § 216.15 or otherwise and (2) the identity of the party to whom the recipient rediscloses the information.

Redisclosure and Reuse of Information Received under an Exception

A recipient's redisclosure of information

A recipient may redisclose nonpublic personal information it receives under an exception in § 216.14 or § 216.15

- To the affiliates of the financial institution that provided the information
- To the recipient's own affiliates, provided those affiliates in turn disclose and use the information only to the extent the recipient could
- In accordance with an exception in § 216.14 or § 216.15 in the ordinary course of business to carry out the activity covered by the exception under which the recipient received the information. § 216.11(a)(1), (c).

Thus, if you receive nonpublic personal information under § 216.14 to service a nonaffiliated financial institution's accounts, you may disclose that information under any other exception described in § 216.14 or § 216.15 in order to carry out the business of servicing those accounts. For example, you would be permitted to disclose the information to your auditors or attorneys or in response to an authorized subpoena.

A recipient's reuse of information

A recipient also may use information it receives under an exception, but only in the ordinary course of business to carry out the activity covered by the exception under which it obtained the information. §§ 216.11(a)(1)(iii) and 216.11(c)(3). If another financial institution gives you nonpublic personal information so that you can process a consumer's

transaction, you therefore may use that information to carry out the transaction and to accrue or recognize any incentives or bonuses associated with the transaction. By contrast, you may not use the information for purposes not covered by an exception, such as for your own marketing purposes.

Subsequent redisclosure and reuse by a recipient's affiliates

When a recipient discloses to its own affiliate information it obtained under an exception, the affiliate's disclosure and reuse of the information are subject to the same limitations that apply to the recipient, as discussed above. §§ 216.11(a)(1)(ii) and 216.11(c)(2). Thus, your affiliate could reuse or redisclose information you disclose to it in accordance with the exceptions in § 216.14 or § 216.15 but could not use the information to market its or your products and services.

Redisclosure and Reuse of Information Received Outside an Exception

The Privacy Rule restricts subsequent *disclosures* by the recipient of information received outside an exception but does not limit the recipient's subsequent use of that information. Thus, if a nonaffiliated third party is permitted to disclose nonpublic personal information to you only because a consumer did not opt out (rather than as permitted by an exception), you may use the information for your own purposes, including marketing your products and services.

Redisclosure by the recipient to affiliates

A recipient may redisclose information it receives outside an exception

- To the affiliates of the financial institution that provided the information
- To its own affiliates, provided they in turn redisclose the information only to the extent that the recipient could. §§ 216.11(b)(1)(i)-(ii) and 216.11(d)(1)-(2).

Redisclosure by the recipient to other nonaffiliated third parties

When redisclosing nonpublic personal information received outside an exception other than as described above in the preceding section, the recipient essentially "steps into the shoes" of the financial institution that provided the information and may redisclose that information only to the extent that the financial institution would be permitted to disclose the information directly. Thus, you may redisclose information you receive outside an exception in accordance with an exception in § 216.14 or § 216.15. You may redisclose the information to a nonaffiliated third party outside an exception, if your disclosure is consistent with the privacy notice of, and opt-out directions received by, the original financial institution that provided the information. You are bound by a consumer's opt-out direction to the original financial institution even if he or she opts out after you received nonpublic personal information about him or her. Consequently, when you receive nonpublic personal information outside an exception and want to redisclose it to another nonaffiliated third party outside an exception, you must monitor future opt-out elections by the consumers whose information you possess.

Subsequent redisclosure and reuse by a recipient's affiliate

When you redisclose to your affiliate nonpublic personal information you received outside an exception, your affiliate in turn may redisclose that information only in accordance with the two preceding sections and may use the information for its own marketing purposes.