Regulation P
Privacy of Consumer Financial Information

Background

Regulation P, Privacy of Consumer Financial Information, implements the privacy provisions of the Gramm–Leach–Bliley Act for state member banks. Generally, the act, which was signed into law in November 1999 and took effect in November 2000,

- Prohibits financial institutions from disclosing nonpublic personal information about consumers to nonaffiliated third parties, (1) unless the institution satisfies various notice and opt-out requirements and (2) provided that the consumer has not elected to opt out of the disclosure
- Requires institutions to provide notice of its privacy policies and practices to its customers

Regulation P establishes rules governing the duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information. Compliance with the rules has been required since July 1, 2001. Generally, a financial institution

- Must provide a notice of its privacy policies to consumers and allow consumers to opt out of the disclosure of their nonpublic personal information to nonaffiliated third parties (subject to certain exceptions) if the disclosure is outside of the exceptions
- Must provide a notice of its privacy policies to its customers, whether or not the institution shares nonpublic personal information
- May not disclose customer account numbers to any nonaffiliated third party for marketing purposes
- Must follow reuse and redisclosure limitations on any nonpublic personal information it receives from nonaffiliated financial institutions

Scope

Regulation P applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes. It does not apply to businesses or to individuals who obtain financial products or services for business, commercial, or agricultural purposes.

Definitions and Key Concepts

Regulation P employs a number of key concepts when discussing the duties and limitations imposed by the regulation. These concepts are briefly discussed below. A more complete explanation of each appears in the regulation.

Financial Institution

A *financial institution* is any institution whose business is engaging in activities that are financial in nature or incidental to such financial activities, as determined by section 4(k) of the Bank Holding Company Act of 1956. Financial institutions can include banks, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents.[1]

Nonpublic Personal Information

Generally, *nonpublic personal information* is any financial information that is personally identifiable and not publicly available, including information that

- A consumer provides to a financial institution to obtain a financial product or service from the institution
- Results from a transaction between the consumer and the institution involving a financial product or service
- A financial institution otherwise obtains about a consumer in connection with providing a financial product or service

Information is considered *publicly available* if the institution has a reasonable basis for believing that the general public may lawfully access the information from government records, widely distributed media, or legally required disclosures to the general public. Examples include information listed in a telephone book or a publicly recorded document, such as a mortgage or securities filing.

Nonpublic personal information may include individual items of information as well as lists of information. For example, names, addresses, phone numbers, Social Security numbers, income, credit scores, and information obtained through Internet collection devices (that is, cookies) may be nonpublic information.

Regulation P includes special rules for lists. Publicly available information is considered nonpublic if it is derived from a source of nonpublic

1. Certain functionally regulated subsidiaries, such as brokers, dealers, and investment advisers, are subject to privacy regulations issued by the Securities and Exchange Commission. Insurance entities may be subject to privacy regulations issued by their respective state insurance authorities.

personal information. For example, a list of the names and addresses of a financial institution's depositors derived from the financial institution's records (which are not publicly available) would be considered nonpublic personal information even though the names and addresses of these individuals might be published in local telephone directories.

However, if the financial institution has a reasonable basis for believing that certain customer relationships are a matter of public record, then any list of these relationships would be considered publicly available information. For instance, a list of mortgage customers whose mortgages are recorded in public records would be considered publicly available information. The institution could provide a list of such customers, and include on the list any other publicly available information it has about those customers, without having to provide to its customers a notice or the possibility of opting out.

Nonaffiliated Third Party

A *nonaffiliated third party* is any person, except a financial institution's affiliate or a person employed jointly by a financial institution and a company, that is not the institution's affiliate. An *affiliate* of a financial institution is any company that controls, is controlled by, or is under common control with the financial institution.

Opt-Out Right and Exceptions

Opt-Out Right

With certain exceptions, consumers must be given the right to *opt out* of the disclosure of their nonpublic personal information—that is, to prevent a financial institution from disclosing nonpublic personal information about them to a nonaffiliated third party—including a reasonable opportunity and a reasonable means of opting out. What constitutes a *reasonable opportunity to opt out* depends on the circumstances surrounding the consumer's transaction, but a consumer must be provided a reasonable amount of time to exercise the opt-out right. For example, thirty days from the date a notice is mailed or a customer acknowledges receipt of an electronic notice would be a reasonable amount of time for the customer to return an opt-out direction.

A *reasonable means to opt out* may include a check-off box, a reply form, or a toll-free telephone number, again depending on the circumstances surrounding the consumer's transaction. It is not reasonable to require a consumer to write his or her own letter as the only means of opting out.

Exceptions

Exceptions to the opt-out right are detailed in sections 13, 14, and 15 of Regulation P. Financial institutions need not comply with opt-out requirements if they limit their disclosure of nonpublic personal information

- To a nonaffiliated third party to perform services for the financial institution or to function on its behalf, including marketing the institution's own products or services or those offered jointly by the institution and another financial institution. The exception is permitted only if the financial institution provides notice of these arrangements and by contract prohibits the third party from disclosing or using the information for other than the specified purposes. The contract must provide that the parties to the agreement are jointly offering, sponsoring, or endorsing a financial product or service. However, if the service or function is covered by the exceptions in section 14 or 15 (discussed below), the financial institution does not have to comply with the additional disclosure and confidentiality requirements of section 13. Disclosure under this exception could include the outsourcing of marketing to an advertising company. (section 13)
- As necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or under certain other circumstances relating to existing relationships with customers. Disclosures under this exception could be in connection with the audit of credit information or the administration of a rewards program or to provide an account statement. (section 14)
- For specified other disclosures that a financial institution normally makes, such as to protect against or prevent actual or potential fraud; to the financial institution's attorneys, accountants, and auditors; or to comply with applicable legal requirements, such as the disclosure of information to regulators. (section 15)

Consumer and Customer

The distinction between consumers and customers is significant because financial institutions have additional disclosure duties with respect to customers. All customers covered by the regulation are consumers, but not all consumers are customers.

A *consumer* is an individual, or that individual's legal representative, who obtains or has obtained from a financial institution a financial product or service that is to be used primarily for personal, family, or household purposes. A *financial service* includes a financial institution's evaluation of or brokerage of information that the institution collects in connection with a request or an application from

a consumer for a financial product or service. For example, a financial service includes a lender's evaluation of an application for a consumer loan or for opening a deposit account, even if the application is ultimately rejected or withdrawn.

A *customer* is a consumer who has a customer relationship with a financial institution. A *customer relationship* is a *continuing* relationship between a consumer and a financial institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. For example, a customer relationship may be established when a consumer engages in one of the following activities with a financial institution:

- Maintains a deposit or investment account
- Obtains a loan
- Enters into a lease of personal property
- Obtains financial, investment, or economic advisory services for a fee

Customers are entitled to receive an initial and an annual privacy notice regardless of the information-disclosure practices of their financial institution.

Consumers who are not customers are entitled to an initial privacy and opt-out notice only if the financial institution wants to share their nonpublic personal information with nonaffiliated third parties outside of the exceptions.

There is a special rule for loans. When a financial institution sells the servicing rights for a loan to another financial institution, the customer relationship transfers with the servicing rights. However, if the institution sells the servicing rights, any information the institution retains about the borrower must be accorded the protections due any consumer.

Note that isolated transactions alone will not cause a consumer to be treated as a customer. For example, if an individual purchases a bank check from a financial institution at which he or she does not have an account, the individual is a consumer but not a customer of that institution because he or she has not established a customer relationship. Likewise, if an individual uses the ATM of a financial institution at which he or she has no account, even uses that ATM repeatedly, the individual is a consumer but is not a customer of that institution.

Financial Institution Duties

Regulation P establishes specific duties and limitations for a financial institution according to its activities. Institutions that intend to disclose nonpublic personal information outside the exceptions must provide opt-out rights to their customers and to consumers who are not customers. All financial institutions must provide an initial and annual notice of their privacy policies to their customers. And all institutions must abide by the regulatory limits on the disclosure of account numbers to nonaffiliated third parties and on the redisclosure and reuse of nonpublic personal information received from nonaffiliated financial institutions. A summary of financial institution duties and limitations follows.

Notice and Opt-out Duties to Consumers

If a financial institution intends to disclose nonpublic personal information about any of its consumers (whether or not they are customers) to a nonaffiliated third party and an exception does not apply, the institution must provide to the consumer

- An initial notice of its privacy policies
- An opt-out notice (including, among other things, a reasonable means of opting out)
- A reasonable opportunity, before the institution discloses the information to the nonaffiliated third party, to opt out

Generally, a financial institution may not disclose any nonpublic personal information to nonaffiliated third parties unless these notices have been provided *and* the consumer has not opted out. Additionally, the institution must provide a *revised notice* before it begins to share a new category of nonpublic personal information or shares information with a new category of nonaffiliated third parties in a manner that was not described in the previous notice.

Note that a financial institution need not comply with the initial and opt-out notice requirements for consumers who are not customers if the institution limits disclosure of nonpublic personal information to the exceptions.

Notice Duties to Customers

In addition to the duties to consumers described in the preceding section, financial institutions have several duties specifically to customers. In particular, regardless of whether the institution discloses or intends to disclose nonpublic personal information, it must provide notice to its customers of its privacy policies and practices at various times. Briefly, a financial institution

- Must provide an *initial notice* of its privacy policies and practices to each customer, no later than the time a customer relationship is established. Instances in which the notice may be provided *after* the customer relationship has

been established are described in section 4(e) of the regulation.

- Must provide an *annual notice* at least once in any period of twelve consecutive months during the continuation of the customer relationship
- Must provide a *new notice* to an existing customer when the customer obtains a new financial product or service from the institution if the initial or annual notice most recently provided to the customer was *not* accurate with respect to the new financial product or service
- Has the option of providing a simplified notice when the institution does not disclose nonpublic personal information (other than as permitted under section 14 and section 15 exceptions) and does not reserve the right to do so

Requirements for Notices

Clear and Conspicuous

Privacy notices must be clear and conspicuous, meaning that they must be reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. While the regulation does not prescribe specific methods for making a notice clear and conspicuous, it does suggest ways in which to achieve the standard, such as using short explanatory sentences or bullet lists, plain-language headings, and easily readable typefaces and type sizes. Privacy notices also must accurately reflect the institution's privacy practices.

Delivery Rules

Privacy notices must be provided so that each recipient can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically. To meet this standard, a financial institution could, for example, (1) hand-deliver a printed copy of the notice to a consumer, (2) mail a printed copy of the notice to the consumer's last known address, or (3) for consumers who conduct transactions electronically, post the notice on the institution's web site and require the consumer to acknowledge receipt of the notice before completing the transaction.

For customers only, a financial institution must provide the initial notice (as well as the annual notice and any revised notice) so that a customer can retain or subsequently access the notice. A written notice satisfies this requirement. For customers who obtain financial products or services electronically and agree to receive their notices on the institution's web site, the institution may provide the current version of its privacy notice on its web site.

Notice Content

A privacy notice must contain specific disclosures. However, a financial institution may provide consumers who are not customers a ''short form'' initial notice together with an opt-out notice (1) stating that the institution's privacy notice is available upon request and (2) explaining a reasonable means for the consumer to obtain it. The following information regarding nonpublic personal information must be provided in privacy notices, as applicable:

- Categories of information collected
- Categories of information disclosed
- Categories of affiliates and nonaffiliated third parties to whom the institution may disclose information
- Policies with respect to the treatment of former customers' information
- Information disclosed to service providers and joint marketers (section 13)
- Explanation of the opt-out right and methods of opting out
- Any opt-out notices the institution must provide under the Fair Credit Reporting Act with respect to affiliate information sharing
- Policies for protecting the security and confidentiality of information
- A statement that the institution makes disclosures to other nonaffiliated third parties as permitted by law (sections 14 and 15)

Limitations on Disclosure of Account Numbers

A financial institution must not disclose an account number or similar form of access number or access code for a credit card, deposit account, or transaction account to any nonaffiliated third party (other than a consumer reporting agency) for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. Encrypted account numbers without an accompanying means of decryption, however, are not subject to this prohibition.

The regulation also expressly allows financial institutions to disclose account numbers to an agent to market the institution's own products or services (although the institution must not authorize the agent to initiate charges to the customer's account). Also not barred are disclosures to participants in private-label or affinity card programs, for which the participants are identified to the customer when the customer enters the program.

Redisclosure and Reuse Limitations on Nonpublic Personal Information Received

If a financial institution receives nonpublic personal information from a nonaffiliated financial institution, the disclosure and use of this information is limited.

- For nonpublic personal information received under a section 14 or 15 exception, the financial institution is limited to
  - Disclosing the information to the affiliates of the financial institution from which it received the information
  - Disclosing the information to its own affiliates, who may, in turn, disclose and use the information only to the extent that the financial institution may do so
  - Disclosing and using the information to carry out the activities covered by a section 14 or 15 exception (for example, an institution receiving information for account processing could disclose the information to its auditors)
- For nonpublic personal information not received under a section 14 or 15 exception, the recipient's use of the information is unlimited, but its disclosure of the information is limited to
  - Disclosing the information to the affiliates of the financial institution from which it received the information
  - Disclosing the information to its own affiliates, who may, in turn disclose the information only to the extent that the financial institution may do so
  - Disclosing the information to any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which it received the information. For example, an institution that received a customer list from another financial institution could disclose the list (1) in accordance with the privacy policy of the financial institution that provided the list, (2) subject to any opt-out election or revocation by the consumers on the list, and (3) in accordance with appropriate exceptions under sections 14 and 15.

Other Matters

Fair Credit Reporting Act

Regulation P does not modify, limit, or supersede the operation of the Fair Credit Reporting Act.

State Law

Regulation P does not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that it is inconsistent with the regulation. A state statute, regulation, order, or other interpretation is consistent with the regulation if it affords any consumer greater protection than that provided under the regulation, as determined by the Federal Trade Commission.

Grandfathered Service Contracts

Contracts that a financial institution entered into on or before July 1, 2000, with a nonaffiliated third party to perform services for the financial institution or functions on its behalf, as described in section 13, satisfied the confidentiality requirements of section 13(a)(1)(ii) until July 1, 2002, even if the contract did not include a requirement that the third party maintain the confidentiality of nonpublic personal information.

Guidelines for Protecting Customer Information

Regulation P requires a financial institution to disclose its policies and practices for protecting the confidentiality, security, and integrity of nonpublic personal information about consumers (whether or not they are customers). The disclosure need not describe these policies and practices in detail. Instead, the disclosures may describe in general terms who is authorized to have access to the information and whether the institution has security practices and procedures in place to ensure the confidentiality of the information in accordance with the institution's policies.

The FFIEC (Federal Financial Institutions Examination Council) has published guidelines, pursuant to section 501(b) of the Gramm–Leach–Bliley Act, that address the steps a financial institution should take in order to protect customer information. The guidelines relate only to information about customers, rather than all consumers. Compliance examiners should consider the findings of a 501(b) inspection during the compliance examination of a financial institution for purposes of evaluating the accuracy of the institution's disclosure regarding data security.

Regulation P
Examination Objectives and Initial Examination Procedures

EXAMINATION OBJECTIVES

1. To assess the quality of a financial institution's compliance management policies and procedures for implementing Regulation P, specifically, ensuring consistency between what the financial institution tells consumers in its notices about its policies and practices and what it actually does
2. To determine the reliance that can be placed on a financial institution's internal controls and procedures for monitoring the institution's compliance with Regulation P
3. To determine a financial institution's compliance with Regulation P, specifically in meeting the following requirements:
   - Providing to customers notices of its privacy policies and practices that are timely, accurate, clear and conspicuous, and delivered so that each customer can reasonably be expected to receive actual notice
   - Disclosing nonpublic personal information to nonaffiliated third parties, other than under an exception, after first meeting the applicable requirements for giving consumers notice and the right to opt out
   - Appropriately honoring consumer opt-out directions
   - Lawfully using or disclosing nonpublic personal information received from a nonaffiliated financial institution
   - Disclosing account numbers only according to the limits in the regulation
4. To initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient

INITIAL EXAMINATION PROCEDURES

A. Through discussions with management and review of available information, identify the institution's practices of sharing information with affiliates and nonaffiliated third parties (and changes in those practices); how the institution treats nonpublic personal information; and how it administers opt-outs. Consider the following, as appropriate:
   1. Notices (initial, annual, revised, opt-out, short-form, and simplified)
   2. Institutional privacy policies and procedures, including those to
      - Process requests for nonpublic personal information, including requests for aggregated data
      - Deliver notices to consumers
      - Manage consumer opt-out directions (for example, designating opt-out files, allowing a reasonable time to opt out, providing new opt-out and privacy notices when necessary, receiving opt-out directions, handling joint account holders)
      - Prevent the unlawful disclosure and use of the information received from nonaffiliated financial institutions
      - Prevent the unlawful disclosure of account numbers
   3 Information-sharing agreements between the institution and affiliates as well as service agreements or contracts between the institution and nonaffiliated third parties to obtain or provide information or services
   4. Complaint logs, telemarketing scripts, and any other information obtained from nonaffiliated third parties (Note: Review telemarketing scripts to determine whether the contractual terms set forth under section 13 are met and whether the institution is disclosing account-number information in violation of section 12.)
   5. Categories of nonpublic personal information collected from or about consumers when obtaining a financial product or service (for example, in the application process for deposit, loan, or investment products; for an over-the-counter purchase of a bank check; from e-banking products or services, including the data collected electronically through Internet cookies; or through ATM transactions)
   6. Categories of nonpublic personal information shared with, or received from, each nonaffiliated third party
   7. Consumer complaints regarding the treatment of nonpublic personal information, including complaints received electronically
   8. Records that reflect the bank's categorization of its information-sharing practices under sections 13, 14, and 15 and outside these exceptions
   9. Results of a 501(b) inspection (used to determine the accuracy of the institution's privacy disclosures regarding data security)

B. Use the information gathered via procedure A to work through the "Privacy Notices and Opt-Out

Provisions'' decision tree (appendix A at the end of this chapter). Identify which of the six examination procedures modules is (are) applicable. (The modules follow this set of initial procedures.)

C. Use the information gathered via procedure A to work through the ''Reuse and Redisclosure'' and ''Account-Number Sharing'' decision trees, as necessary (appendixes B and C at the end of this chapter). Identify the applicable examination procedures module(s).

D. Determine the adequacy of the financial institution's internal controls and procedures to ensure compliance with Regulation P. Consider all of the following:
   1. Sufficiency of internal policies, procedures, and controls, including those related to new products and services and controls over servicing arrangements and marketing arrangements
   2. Effectiveness of management information systems, including exception reports, the standardization of forms and procedures, and the use of technology for monitoring
   3. Frequency and effectiveness of monitoring procedures
   4. Adequacy and regularity of the institution's training program
   5. Suitability of the compliance audit program for ensuring that
      - The procedures address all regulatory provisions, as applicable
      - The work is accurate and comprehensive with respect to the institution's information-sharing practices
      - The frequency is appropriate
      - Conclusions are appropriately reached and presented to responsible parties
      - Steps are taken to correct deficiencies and to follow up on previously identified deficiencies
   6. Knowledge level of management and personnel

E. Ascertain areas of risk associated with the financial institution's sharing practices (especially those within section 13 and those that fall outside the exceptions) and any weaknesses found within the compliance management program. Follow up on any outstanding deficiencies identified in the audit when completing the modules.

F. On the basis of the results of the foregoing initial procedures and discussions with management, determine which procedures in the applicable examination procedures module, if any, should be completed, focusing on areas of particular risk. The selection of procedures to be completed depends on the adequacy of the institution's compliance management system and the level of risk identified. Each module contains a set of general instructions for verifying compliance, cross-referenced to cites within the regulation. Each module also contains cross-references to more questions, which the examiner may use if needed to evaluate compliance in more detail.

G. Evaluate any additional information or documentation discovered during the course of the examination according to these procedures. Note that this may reveal new or different sharing practices, necessitating reapplication of the decision trees and completion of additional or different modules.

H. Formulate conclusions.
   1. Summarize all findings.
   2. For violation(s) noted, determine the cause by identifying weaknesses in internal controls, compliance review, training, management oversight, or other areas.
   3. Identify action needed to correct violations and weaknesses in the institution's compliance system, as appropriate.
   4. Discuss findings with management, and obtain a commitment for corrective action.

For reviewing the sharing of nonpublic personal information with nonaffiliated third parties under sections 14 and/or 15 of Regulation P and outside the exceptions (with or without also sharing under section 13)

(Note: Financial institutions whose practices fall within this category engage in the most expansive degree of information sharing permissible. Consequently, these institutions are held to the most comprehensive compliance standards imposed by the privacy regulation.)

A. Disclosure of Nonpublic Personal Information

1. Select a sample of third-party relationships with nonaffiliated third parties, and then a sample of data shared between the institution and the third party both inside and outside the exceptions. The sample should include a cross-section of relationships but should emphasize those that are higher risk in nature as determined by the initial procedures. Make the following comparisons to evaluate the financial institution's compliance with disclosure limitations:
   a. Compare the categories of data shared and the entities with which the data were shared with the categories stated in the privacy notice. Verify that what the institution tells consumers (customers and those who are not customers) in its notices about its policies and practices in this regard is consistent with what the institution actually does. (§§ 216.10 and 6)
   b. Compare the data shared with a sample of opt-out directions and verify that only nonpublic personal information covered under the exceptions, or from consumers (customers and those who are not customers) who chose not to opt out, is shared. (§ 216.10)
2. If the financial institution also shares information under section 13, obtain and review contracts with nonaffiliated third parties that perform services for the financial institution that are not covered by the exceptions in section 14 or 15. Determine whether the contracts prohibit the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Note that the ''grandfather'' provisions of section 18 may apply to certain contracts. (§ 216.13(a))

B. Presentation, Content, and Delivery of Privacy Notices

1. Review the financial institution's initial, annual, and revised notices as well as any short-form notices that the institution may use for consumers who are not customers. Determine whether or not these notices
   a. Are clear and conspicuous (§§ 216.3(b), 4(a), 5(a)(1), and 8(a)(1))
   b. Accurately reflect the institution's policies and practices (§§ 216.4(a), 5(a)(1), and 8(a)(1)) (Note: This includes practices disclosed in the notices that exceed regulatory requirements.)
   c. Include, and adequately describe, all required items of information and contain examples, as applicable (§ 216.6) (Note that if the institution shares information under section 13, the notice provisions for that section also apply.)
2. Through discussions with management, a review of the institution's policies and procedures, and a sample of electronic or written consumer records when available, determine if the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
   a. Timeliness of delivery (§§ 216.4(a), 7(c), and 8(a))
   b. Reasonableness of the method of delivery (for example, by hand; by mail; electronically, if the consumer agrees; or as a necessary step of a transaction) (§ 216.9)
   c. For customers only, review the timeliness of delivery (§§ 216.4(d), 4(e), and 5(a)), the means of delivery of the annual notice (§ 216.9(c)), and the accessibility of or ability to retain the notice (§ 216.9(e)).

C. Opt-Out Right

1. Review the financial institution's opt-out notices. An opt-out notice may be combined with the institution's privacy notices. Regardless, determine whether the opt-out notices
   a. Are clear and conspicuous (§§ 216.3(b) and 7(a)(1))
   b. Accurately explain the right to opt out (§ 216.7(a)(1))
   c. Include and adequately describe the three required items of information (the

institution's policy regarding disclosure of nonpublic personal information, the consumer's opt-out right, and the means to opt out) (§ 216.7(a)(1))

d. Describe how the institution treats joint consumers (customers and those who are not customers), as applicable (§ 216.7(d))

2. Through discussions with management, a review of the institution's policies and procedures, and a sample of electronic or written records where available, determine if the institution has adequate procedures in place to provide the opt-out notice and comply with the opt-out directions of consumers (customers and those who are not customers), as appropriate. Assess the following:

   a. Timeliness of delivery (§ 216.10(a)(1))

   b. Reasonableness of the method of delivery (for example, by hand; by mail; electronically, if the consumer agrees; or as a necessary step of a transaction) (§ 216.9)

   c. Reasonableness of the opportunity to opt out (the time period, and the means by which the consumer may opt out) (§§ 216.10(a)(1)(iii) and 10(a)(3))

   d. Adequacy of procedures to implement and track the status of consumers' (customers and those who are not customers) opt-out directions, including those of former customers (§ 216.7(e), (f), and (g))

D. Checklist Cross-References

Regulation section	*Subject*	*Checklist questions*
216.4(a), 6(a, b, c, e), and 9(a, b, g)	Privacy notices (presentation, content, and delivery)	2, 8–11, 14, 18, 35, 36, and 40
216.4(a, c, d, e), 5, and 9(c, e)	Rules for delivering customer notices	1, 3–7, 37, and 38
216.13	Section 13 notice and contracting rules (as applicable)	12 and 47
216.6(d)	Short-form notice rules (optional for consumers only)	15–17
216.7, 8, and 10	Opt-out rules	19–34 and 41–43
216.14 and 15	Exceptions	48–50

For reviewing the sharing of nonpublic personal information with nonaffiliated third parties under sections 13, 14, and 15 of Regulation P, but not outside these exceptions

A. Disclosure of Nonpublic Personal Information

1. Select a sample of third-party relationships with nonaffiliated third parties, and then a sample of data shared between the institution and the third party. The sample should include a cross-section of relationships but should emphasize those that are higher risk in nature as determined by the initial procedures. Make the following comparisons to evaluate the financial institution's compliance with disclosure limitations:
   a. Review the data shared and the entities with which the data were shared to ensure that the institution accurately categorized its information-sharing practices and is not sharing nonpublic personal information outside the exceptions. (§§ 216.13–15)
   b. Compare the categories of data shared and the entities with which the data were shared with the categories stated in the privacy notice. Verify that what the institution tells consumers in its notices about its policies and practices in this regard is consistent with what the institution actually does. (§§ 216.10 and 6)
2. Review contracts with nonaffiliated third parties that perform services for the financial institution that are not covered by the exceptions in section 14 or 15. Determine whether the contracts adequately prohibit the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Note that the "grandfather" provisions of section 18 apply to certain of these contracts. (§ 216.13(a))

B. Presentation, Content, and Delivery of Privacy Notices

1. Review the financial institution's initial and annual privacy notices. Determine whether or not they
   a. Are clear and conspicuous (§§ 216.3(b), 4(a), and 5(a)(1))
   b. Accurately reflect the institution's policies and practices (§ 216.4(a) and 5(a)(1)) (Note: This includes practices disclosed in the notices that exceed regulatory requirements.)
   c. Include, and adequately describe, all required items of information and contain examples as applicable (§§ 216.6 and 13)
2. Through discussions with management, a review of the institution's policies and procedures, and a sample of electronic or written consumer records when available, determine if the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
   a. Timeliness of delivery (§ 216.4(a))
   b. Reasonableness of the method of delivery (for example, by hand; by mail; electronically, if the consumer agrees; or as a necessary step of a transaction) (§ 216.9)
   c. For customers only, review the timeliness of delivery (§§ 216.4(d), 4(e), and 5(a)), the means of delivery of the annual notice (§ 216.9(c)), and the accessibility of or ability to retain the notice. (§ 216.9(e))

C. Checklist Cross-References

Regulation section	*Subject*	*Checklist questions*
216.4(a), 6(a, b, c, e), and 9(a, b, g)	Privacy notices (presentation, content, and delivery)	2, 8–11, 14, 18, 35, 36, and 40
216.13	Section 13 notice and contracting rules (as applicable)	12 and 47
216.4(a, c, d, e), 5, and 9(c, e)	Rules for delivering customer notices	1, 3–7, 37, and 38
216.14 and 15	Exceptions	48–50

Regulation P
Examination Procedures—Module 3

For reviewing the sharing of nonpublic personal information with nonaffiliated third parties only under sections 14 and 15 of Regulation P

(Note: This module applies only to customers.)

A. Disclosure of Nonpublic Personal Information

1. Select a sample of third-party relationships with nonaffiliated third parties, and then a sample of data shared between the institution and the third party.
2. Review the data shared and the entities with which the data were shared to ensure that the institution accurately states its information-sharing practices and is not sharing nonpublic personal information outside the exceptions.

B. Presentation, Content, and Delivery of Privacy Notices

1. Obtain and review the financial institution's initial and annual notices, as well as any simplified notice the institution may use. Note that the institution may use the simplified notice only when it does not also share nonpublic personal information with affiliates outside section 14 and 15 exceptions. Determine whether or not these notices
   a. Are clear and conspicuous (§§ 216.3(b), 4(a), and 5(a)(1))
   b. Accurately reflect the institution's policies and practices (§§ 216.4(a) and 5(a)(1)) (Note: This includes practices disclosed in the notices that exceed regulatory requirements.)
   c. Include, and adequately describe, all required items of information (§ 216.6)
2. Through discussions with management, a review of the institution's policies and procedures, and a sample of electronic or written customer records when available, determine if the institution has adequate procedures in place to provide notices to customers, as appropriate. Assess the following:
   a. Timeliness of delivery (§§ 216.4(a), 4(d), 4(e), and 5(a))
   b. Reasonableness of the method of delivery (for example, by hand; by mail; electronically, if the customer agrees; or as a necessary step of a transaction) (§ 216.9) and the accessibility of or ability to retain the notice (§ 216.9(e))

C. Checklist Cross-References

Regulation section	*Subject*	*Checklist questions*
216.6	Customer-notice content and presentation	8–11, 14, and 18
216.6(c)(5)	Simplified-notice content (optional)	13
216.4(a, d, e), 5, and 9	Customer-notice delivery process	1, 3–7, and 35–40
216.14 and 15	Exceptions	48–50

Examination Procedures—Module 4

For reviewing the reuse and redisclosure of nonpublic personal information received from a nonaffiliated financial institution under sections 14 and 15 of Regulation P

A. Through discussions with management and a review of the institution's procedures, determine whether the institution has adequate practices in place to prevent the unlawful redisclosure and reuse of information when the institution is the recipient of nonpublic personal information. (§ 216.11(a))

B. Select a sample of data received from nonaffiliated financial institutions to evaluate the financial institution's compliance with reuse and redisclosure limitations.

1. Verify that the institution redisclosed information only to affiliates of the financial institution from which the information was obtained or to the institution's own affiliates, except as otherwise allowed. (§ 216.11(a)(1)(i) and (ii))
2. Verify that the institution uses and shares the data only pursuant to an exception in sections 14 and 15. (§ 216.11(a)(1)(iii))

C. Checklist Cross-References

Regulation section	*Subject*	*Checklist question*
216.11(a)	Reuse and redisclosure	44

Examination Procedures—Module 5

For reviewing the redisclosure of nonpublic personal information received from a nonaffiliated financial institution outside sections 14 and 15 of Regulation P

A. Through discussions with management and a review of the institution's procedures, determine whether the institution has adequate practices in place to prevent the unlawful redisclosure of information when the institution is the recipient of nonpublic personal information. (§ 216.11(b))

B. Select a sample of data received from nonaffiliated financial institutions and shared with others to evaluate the financial institution's compliance with the redisclosure limitations.

   1. Verify that the institution's redisclosure of the information was only to affiliates of the financial institution from which the information was obtained or to the institution's own affiliates, except as otherwise allowed. (§§ 216.11(b)(1)(i) and (ii))
   2. If the institution shares information, verify that the institution's information-sharing practices conform to those in the nonaffiliated financial institution's privacy notice. (§ 216.11(b)(1)(iii))
   3. Also, review the procedures used by the institution to ensure that the information-sharing reflects the opt-out status of the consumers of the nonaffiliated financial institution. (§§ 216.10 and 11(b)(1)(iii))

C. Checklist Cross-References

Regulation section	*Subject*	*Checklist question*
216.11(b)	Reuse and redisclosure	45

Examination Procedures—Module 6

For reviewing the sharing of account numbers

A. If available, review a sample of telemarketing scripts used when making sales calls, to determine whether the scripts indicate that the telemarketers have the account numbers of the institution's consumers. (§ 216.12)

B. Obtain and review a sample of contracts with agents or service providers to whom the financial institution discloses account numbers for use in connection with marketing the institution's own products or services. Determine whether the institution shares account numbers with nonaffiliated third parties only to conduct marketing for the institution's own products and services. Ensure that the contracts do not authorize these nonaffiliated third parties to directly initiate charges to customer's accounts. (§ 216.12(b)(1))

C. Obtain a sample of materials and information provided to the consumer upon entering a private-label or affinity credit card program. Determine if the participants in each program are identified to the customer when the customer enters into the program. (§ 216.12(b)(2))

D. Checklist Cross-References

Regulation section	*Subject*	*Checklist question*
216.12	Account-number sharing	46

Regulation P
Examination Checklist

SUBPART A

Initial Privacy Notice

1. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to *all customers* not later than when the customer relationship is established, other than as allowed in paragraph (e) of section 216.4 of Regulation P? (§ 216.4(a)(1)) Yes No

   Note: No notice is required if nonpublic personal information is disclosed to nonaffiliated third parties only under an exception in sections 216.14 and 15 and there is no customer relationship. (§ 216.4(b)) With respect to credit relationships, an institution establishes a customer relationship when it originates a consumer loan. If the institution subsequently sells the servicing rights to the loan to another financial institution, the customer relationship transfers with the servicing rights. (§ 216.4(c))

2. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to *all consumers* who are not customers before any nonpublic personal information about the consumer is disclosed to a nonaffiliated third party, other than under an exception in section 216.14 or 15? (§ 216.4(a)(2)) Yes No

3. Does the institution provide to *existing customers* who obtain a new financial product or service an initial privacy notice that covers the customer's new financial product or service, if the most recent notice provided to the customer was not accurate with respect to the new financial product or service? (§ 216.4(d)(1)) Yes No

4. *After establishing a customer relationship,* does the institution provide initial notice only under one of the following circumstances?

   a. The customer relationship is not established at the customer's election (§ 216.4(e)(1)(i)) Yes No

   b. To do otherwise would substantially delay the customer's transaction (for example, in the case of a telephone application) and the customer agrees to the subsequent delivery (§ 216.4 (e)(1)(ii)) Yes No

5. When the subsequent delivery of a privacy notice is permitted, does the institution provide notice after establishing a customer relationship within a reasonable time? (§ 216.4(e)) Yes No

Annual Privacy Notice

6. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices at least annually (that is, at least once in any period of 12 consecutive months) to all customers, throughout the customer relationship? (§§ 216.5(a)(1)and (2)) Yes No

   Note: Annual notices are not required for former customers. (§§ 216.5(b)(1) and (2))

7. Does the institution provide an annual privacy notice to each customer for whom the institution owns the loan-servicing rights? (§§ 216.5(c) and 4(c)(2)) Yes No

Content of Privacy Notices

8. Do the initial, annual, and revised privacy notices include each of the following, as applicable?
   a. The categories of nonpublic personal information that the institution collects (§ 216.6(a)(1)) Yes No
   b. The categories of nonpublic personal information that the institution discloses (§ 216.6(a)(2)) Yes No
   c. The categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information, other than parties to whom information is disclosed under an exception in section 216.14 or 15 (§ 216.6(a)(3)) Yes No
   d. The categories of nonpublic personal information disclosed about former customers, and the categories of affiliates and nonaffiliated third parties to whom the institution discloses that information, other than those parties to whom the institution discloses information under an exception in section 216.14 or 15 (§ 216.6(a)(4)) Yes No
   e. If the institution discloses nonpublic personal information to a nonaffiliated third party under section 216.13 and no exception under section 216.14 or 15 applies, a separate statement of the categories of information the institution discloses and the categories of third parties with whom the institution has contracted (§ 216.6(a)(5)) Yes No
   f. An explanation of the opt-out right, including the method(s) of opting out that the consumer may use at the time of the notice (§ 216.6(a)(6)) Yes No
   g. Any disclosures the institution makes under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (§ 216.6(a)(7)) Yes No
   h. The institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (§ 216.6(a)(8)) Yes No
   i. A general statement—with no specific reference to the exceptions or to the third parties—that the institution makes disclosures to other nonaffiliated third parties as permitted by law (§§ 216.6(a)(9) and (b)) Yes No

   Note: Sample clauses for these items appear in appendix A to Regulation P.

9. Does the institution list the following categories of nonpublic personal information that it collects, as applicable?
   a. Information from the consumer (§ 216.6(c)(1)(i)) Yes No
   b. Information about the consumer's transactions with the institution or its affiliates (§ 216.6(c)(1)(ii)) Yes No
   c. Information about the consumer's transactions with nonaffiliated third parties (§ 216.6(c)(1)(iii)) Yes No
   d. Information from a consumer reporting agency (§ 216.6(c)(1)(iv)) Yes No

10. Does the institution list the following categories of nonpublic personal information that it discloses, as applicable, and a few examples of each or, alternatively, state that it reserves the right to disclose all the nonpublic personal information that it collects?
    a. Information from the consumer Yes No
    b. Information about the consumer's transactions with the institution or its affiliates Yes No
    c. Information about the consumer's transactions with nonaffiliated third parties Yes No

d. Information from a consumer reporting agency (§ 216.6(c)(2)) Yes No

Note: Examples are recommended under section 216.6(c)(2), although not under section 216.6(c)(1).

11. Does the institution list the following categories of affiliates and nonaffiliated third parties to whom it discloses information, as applicable, and a few examples to illustrate the types of third parties in each category?

a. Financial service providers (§ 216.6(c)(3)(i)) Yes No

b. Nonfinancial companies (§ 216.6(c)(3)(ii)) Yes No

c. Others (§ 216.6(c)(3)(iii)) Yes No

12. Does the institution make the following disclosures regarding service providers and joint marketers to whom it discloses nonpublic personal information under section 216.13?

a. As applicable, the same categories and examples of nonpublic personal information disclosed as described in paragraphs (a)(2) and (c)(2) of section 216.6 (see questions 8b and 10) (§ 216.6(c)(4)(i)) Yes No

b. That the third party is a service provider that performs marketing on the institution's behalf or on behalf of the institution and another financial institution or (§ 216.6(c)(4)(ii)(A)) Yes No

c. That the third party is a financial institution with which the institution has a joint marketing agreement (§ 216.6(c)(4)(ii)(B)) Yes No

13. If the institution does not disclose nonpublic personal information and does not reserve the right to do so, other than under exceptions in sections 216.14 and 15, does the institution provide a simplified privacy notice that contains, at a minimum, all of the following?

a. A statement to this effect Yes No

b. The categories of nonpublic personal information it collects Yes No

c. The policies and practices the institution uses to protect the confidentiality and security of nonpublic personal information Yes No

d. A general statement that the institution makes disclosures to other nonaffiliated third parties as permitted by law (§ 216.6(c)(5)) Yes No

Note: Use of this type of simplified notice is optional; an institution may always use a full notice.

14. Does the institution describe the following about its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information?

a. Who is authorized to have access to the information (§ 216.6(c)(6)(i)) Yes No

b. Whether security practices and policies are in place to ensure the confidentiality of the information in accordance with the institution's policy (§ 216.6(c)(6)(ii)) Yes No

Note: The institution is not required to describe technical information about the safeguards used in this respect.

15. If the institution provides a short-form initial privacy notice with the opt-out notice, does the institution do so only to consumers with whom the institution does not have a customer relationship? (§ 216.6(d)(1)) Yes No

16. If the institution provides a short-form initial privacy notice according to section 216.6(d)(1), does the short-form initial notice

a. Conform to the definition of ''clear and conspicuous,'' (§ 216.6(d)(2)(i)) Yes No

b. State that the institution's full privacy notice is available upon request and, (§ 216.6(d)(2)(ii)) Yes No

c. Explain a reasonable means by which the consumer may obtain the notice (§ 216.6(d)(2)(iii)) Yes No

Note: The institution is not required to deliver the full privacy notice with the short-form initial notice. (§ 216.6(d)(3))

17. Does the institution provide consumers who receive the short-form initial notice with a reasonable means of obtaining the longer initial notice, such as

a. A toll-free telephone number that the consumer may call to request the notice or (§ 216.6(d)(4)(i)) Yes No

b. Copies available for immediate hand-delivery to consumers who conduct business in person at the institution's office (§ 216.6(d)(4)(ii)) Yes No

18. If the institution, in its privacy policies, reserves the right to disclose nonpublic personal information to nonaffiliated third parties in the future, does the privacy notice include the following, as applicable?

a. Categories of nonpublic personal information that the institution reserves the right to disclose in the future but does not currently disclose and (§ 216.6(e)(1)) Yes No

b. Categories of affiliates or nonaffiliated third parties to whom the institution reserves the right in the future to disclose, but to whom it does not currently disclose, nonpublic personal information (§ 216.6(e)(2)) Yes No

Opt-Out Notice

19. If the institution discloses nonpublic personal information about a consumer to a nonaffiliated third party and the exceptions under sections 216.13–15 do not apply, does the institution provide the consumer with a clear and conspicuous opt-out notice that accurately explains the right to opt out? (§ 216.7(a)(1)) Yes No

20. Does the opt-out notice state the following?

a. That the institution discloses or reserves the right to disclose nonpublic personal information about the consumer to a nonaffiliated third party (§ 216.7(a)(1)(i)) Yes No

b. That the consumer has the right to opt out of that disclosure (§ 216.7(a)(1)(ii)) Yes No

c. A reasonable means by which the consumer may opt out (§ 216.7(a)(1)(iii)) Yes No

21. Does the institution provide the consumer with the following information about the right to opt out?

a. All the categories of nonpublic personal information that the institution discloses or reserves the right to disclose (§ 216.7(a)(2)(i)(A)) Yes No

b. All the categories of nonaffiliated third parties to whom the information is disclosed (§ 216.7(a)(2)(i)(A)) Yes No

c. That the consumer has the right to opt out of the disclosure of that information (§ 216.7(a)(2)(i)(A)) Yes No

d. The financial products or services that the consumer obtains to which the opt-out direction would apply (§ 216.7(a)(2)(i)(B)) Yes No

22. Does the institution provide the consumer with at least one of the following reasonable means of opting out, or with another reasonable means?

a. Check-off boxes prominently displayed on the relevant forms with the opt-out notice (§ 216.7(a)(2)(ii)(A)) Yes No

b. A reply form included with the opt-out notice (§ 216.7(a)(2)(ii)(B)) Yes No

c. An electronic means to opt out, such as a form that can be sent via electronic mail or a process at the institution's web site, if the consumer agrees to the electronic delivery of information (§ 216.7(a)(2)(ii)(C)) Yes No

d. A toll-free telephone number (§ 216.7(a)(2)(ii)(D)) Yes No

Note: The institution may require the consumer to use one specific means of opting out, as long as that means is reasonable for that consumer. (§ 216.7(a)(iv))

23. If the institution delivers the opt-out notice after the initial notice, does the institution provide the initial notice once again with the opt-out notice? (§ 216.7(c)) Yes No

24. Does the institution provide an opt-out notice, to at least one party in a joint consumer relationship, explaining how the institution will treat opt-out directions by the joint consumers? (§ 216.7(d)(1)) Yes No

25. Does the institution permit each of the joint consumers in a joint relationship to opt out? (§ 216.7(d)(2)) Yes No

26. Does the opt-out notice to joint consumers state that either

a. The institution will consider an opt-out by a joint consumer as applying to all associated joint consumers or (§ 216.7(d)(2)(i)) Yes No

b. Each joint consumer is permitted to opt out separately (§ 216.7(d)(2)(ii)) Yes No

27. If each joint consumer may opt out separately, does the institution permit

a. One joint consumer to opt out on behalf of all of the joint consumers, (§ 216.7(d)(3)) Yes No

b. The joint consumers to notify the institution in a single response, and (§ 216.7(d)(5)) Yes No

c. Each joint consumer to opt out for himself or herself or for another joint consumer (§ 216.7(d)(5)) Yes No

28. Does the institution refrain from requiring all joint consumers to opt out before implementing any opt-out direction with respect to the joint account? (§ 216.7(d)(4)) Yes No

29. Does the institution comply with a consumer's direction to opt out as soon as is reasonably practicable after receiving it? (§ 216.7(e)) Yes No

30. Does the institution allow the consumer to opt out at any time? (§ 216.7(f)) Yes No

31. Does the institution continue to honor the consumer's opt-out direction until revoked by the consumer in writing or, if the consumer agrees, electronically? (§ 216.7(g)(1)) Yes No

32. When a customer relationship ends, does the institution continue to apply the customer's opt-out direction to the nonpublic personal information collected during, or related to, that specific customer relationship (but not to new relationships, if any, subsequently established by that customer)? (§ 216.7(g)(2)) Yes No

Revised Notices

33. Except as permitted by sections 216.13–15, does the institution refrain from disclosing any nonpublic personal information about a consumer to a nonaffiliated third party, other than as described in the initial privacy notice provided to the consumer, unless

a. The institution has provided the consumer with a clear and conspicuous revised notice that accurately describes the institution's privacy policies and practices, (§ 216.8(a)(1)) Yes No

b. The institution has provided the consumer with a new opt-out notice, (§ 216.8(a)(2)) Yes No

c. The institution has given the consumer a reasonable opportunity to opt out of the disclosure, before disclosing any information, and (§ 216.8(a)(3)) Yes No

d. The consumer has not opted out (§ 216.8(a)(4)) Yes No

34. Does the institution deliver a revised privacy notice when it does any one of the following?

a. Discloses a new category of nonpublic personal information to a nonaffiliated third party (§ 216.8(b)(1)(i)) Yes No

b. Discloses nonpublic personal information to a new category of nonaffiliated third party (§ 216.8(b)(1)(ii)) Yes No

c. 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 (§ 216.8(b)(1)(iii)) Yes No

Note: A revised notice is not required if the institution adequately described the nonaffiliated third party or information to be disclosed in the prior privacy notice. (§ 216.8(b)(2))

Delivery Methods

35. Does the institution deliver the privacy and opt-out notices, including the short-form notice, so that the consumer can reasonably be expected to receive the actual notice in writing or, if the consumer agrees, electronically? (§ 216.9(a)) Yes No

36. Does the institution use a reasonable means for delivering the notices, such as the following?

a. Hand-delivery of a printed copy (§ 216.9(b)(1)(i)) Yes No

b. Mailing a printed copy to the last known address of the consumer (§ 216.9(b)(1)(ii)) Yes No

c. For the consumer who conducts transactions electronically, posting the notice clearly and conspicuously on the institution's electronic site and requiring the consumer to acknowledge receipt as a necessary step to obtaining a financial product or service (§ 216.9(b)(1)(iii)) Yes No

d. For isolated transactions, such as ATM transactions, posting the notice on the screen and requiring the consumer to acknowledge receipt as a necessary step to obtaining the financial product or service (§ 216.9(b)(1)(iv)) Yes No

Note: Insufficient or unreasonable means of delivery include exclusively oral notice, in person or by telephone; branch or office signs or generally published advertisements; and electronic mail to a customer who does not obtain products or services electronically. (§§ 216.9(b)(2)(i) and (ii) and 216.9(d))

37. For annual notices only, if the institution does not employ one of the methods described in question 36, does the institution employ one of the following reasonable means of delivering the notice?

a. For the customer who uses the institution's web site to access products and services electronically and who agrees to receive notices at the web site, continuously posting the current privacy notice on the web site in a clear and conspicuous manner (§ 216.9(c)(1)) Yes No

b. For the customer who has requested that the institution refrain from sending any information about the customer relationship, making copies of the current privacy notice available upon customer request (§ 216.9(c)(2)) Yes No

38. For customers only, does the institution ensure that the initial, annual, and revised notices can be retained or obtained later by the customer in writing or, if the customer agrees, electronically? (§ 216.9(e)(1)) Yes No

39. Does the institution use an appropriate means to ensure that notices can be retained or obtained later, such as one of the following?

a. Hand-delivery of a printed copy of the notice (§ 216.9(e)(2)(i)) Yes No

b. Mailing a printed copy to the last known address of the customer (§ 216.9(e)(2)(ii)) Yes No

c. Making the current privacy notice available on the institution's web site (or via a link to the notice at another site) for the customer who agrees to receive the notice at the web site (§ 216.9(e)(2)(iii)) Yes No

40. Does the institution provide at least one initial, annual, and revised notice, as applicable, to joint consumers? (§ 216.9(g)) Yes No

SUBPART B

Limits on Disclosure to Nonaffiliated Third Parties

41. Does the institution refrain from disclosing any nonpublic personal information about a consumer to a nonaffiliated third party, other than as permitted under sections 216.13–15, unless all of the following have occurred?

a. It has provided the consumer with an initial notice. (§ 216.10(a)(1)(i)) Yes No

b. It has provided the consumer with an opt-out notice. (§ 216.10(a)(1)(ii)) Yes No

c. It has given the consumer a reasonable opportunity to opt out before the disclosure. (§ 216.10(a)(1)(iii)) Yes No

d. The consumer has not opted out. (§ 216.10(a)(1)(iv)) Yes No

Note: This disclosure limitation applies to consumers as well as to customers (§ 216.10(b)(1)), and to all nonpublic personal information regardless of whether it was collected before or after receiving an opt-out direction. (§ 216.10(b)(2))

42. Does the institution provide the consumer with a reasonable opportunity to opt out, such as by one of the following?

a. Mailing the notices required by section 216.10 and allowing the consumer to respond by toll-free telephone number, return mail, or other reasonable means (see question 22) within 30 days from the date mailed (§ 216.10(a)(3)(i)) Yes No

b. Where the consumer opens an online account with the institution and agrees to receive the notices required by section 216.10 electronically, allowing the consumer to opt out by any reasonable means (see question 22) within 30 days from consumer acknowledgement of receipt of the notice in conjunction with opening the account (§ 216.10(a)(3)(ii)) Yes No

c. For isolated transactions, providing the notices required by section 216.10 at the time of the transaction and requesting that the consumer decide, as a necessary part of the transaction, whether to opt out before completion of the transaction (§ 216.10(a)(3)(iii)) Yes No

43. Does the institution allow the consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out? (§ 216.10(c)) Yes No

Note: An institution may allow partial opt-outs in addition to, but may not allow them instead of, a comprehensive opt-out.

Limits on Redisclosure and Reuse of Information

44. If the institution receives information from a nonaffiliated financial institution under an exception in section 216.14 or 15, does the institution refrain from using or disclosing the information except under the following circumstances?

a. Disclosure to the affiliates of the financial institution from which it received the information (§ 216.11(a)(1)(i)) Yes No

b. Disclosure to its own affiliates, which are in turn limited by the same disclosure and use restrictions as the recipient institution (§ 216.11(a)(1)(ii)) Yes No

c. Disclosure and use of the information pursuant to an exception in section 216.14 or 15 in the ordinary course of business to carry out the activity covered by the exception under which the information was received (§ 216.11(a)(1)(iii)) Yes No

Note: The disclosure or use described in part c of this question need not be directly related to the activity covered by the applicable exception. For instance, an institution receiving information for fraud-prevention purposes could provide the information to its auditors. But ''in the ordinary course of business'' does not include marketing. (§ 216.11(a)(2))

45. If the institution receives information from a nonaffiliated financial institution other than under an exception in section 216.14 or 15, does the institution refrain from disclosing the information except under the following circumstances?

a. To the affiliates of the financial institution from which it received the information (§ 216.11(b)(1)(i)) Yes No

b. To its own affiliates, which are in turn limited by the same disclosure restrictions as the recipient institution (§ 216.11(b)(1)(ii)) Yes No

c. To any other person, if the disclosure would be lawful if made directly to that person by the institution from which the recipient institution received the information (§ 216.11(b)(1)(iii)) Yes No

Limits on Sharing Account-Number Information for Marketing Purposes

46. Does the institution refrain from disclosing, directly or through affiliates, account numbers or similar forms of access numbers or access codes for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party (other than to a consumer reporting agency) for telemarketing, direct mail, or electronic mail marketing to the consumer, except under the following circumstances?

a. To the institution's agents or service providers solely to market the institution's own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account (§ 216.12(b)(1)) Yes No

b. To a participant in a private-label credit card program or an affinity or similar program in which the participants in the program are identified to the customer when the customer enters into the program (§ 216.12(b)(2)) Yes No

Note: An ''account number or similar form of access number or access code'' does not include numbers in encrypted form, so long as the institution does not provide the recipient with a means of decryption. (§ 216.12(c)(1)) A transaction account does not include an account to which third parties cannot initiate charges. (§ 216.12(c)(2))

SUBPART C

Exception to Opt-Out Requirements for Service Providers and Joint Marketing

47. If the institution discloses nonpublic personal information to a nonaffiliated third party without permitting the consumer to opt out, do the opt-out requirements of sections 216.7 and 10 and the revised notice requirements in section 216.8 not apply because

a. The institution disclosed the information to a nonaffiliated third party who performs services for, or functions on behalf of, the institution (including joint marketing of financial products and services offered pursuant to a joint agreement as defined in paragraph (b) of section 216.13), (§ 216.13(a)(1)) Yes No

b. The institution has provided consumers with the initial notice, and (§ 216.13(a)(1)(i)) Yes No

c. The institution has entered into a contract with that party prohibiting the party from disclosing or using the information except to carry out the purposes for which the information was disclosed, including use under an exception in section 216.14 or 15 in the ordinary course of business to carry out those purposes (§ 216.3(a)(1)(ii)) Yes No

Exceptions to Notice and Opt-Out Requirements for Processing and Servicing Transactions

48. If the institution discloses nonpublic personal information to nonaffiliated third parties, do certain requirements—for initial notice in section 216.4(a)(2); opt-out in sections 216.7 and 10; revised notice in section 216.8; and service providers and joint marketing in section 216.13—not apply because the information is disclosed as necessary to effect, administer, or enforce a transaction that the consumer requests or authorizes, or in connection with any of the following?

a. Servicing or processing a financial product or service requested or authorized by the consumer (§ 216.14(a)(1)) Yes No

b. Maintaining or servicing the consumer's account with the institution or with another entity as part of a private-label credit card program or other credit extension on behalf of the entity (§ 216.14(a)(2)) Yes No

c. Effecting a proposed or actual securitization, secondary-market sale (including sale of servicing rights), or other, similar transaction related to a transaction of the consumer (§ 216.14(a)(3)) Yes No

49. If the institution uses a section 216.14 exception as necessary to effect, administer, or enforce a transaction, is the disclosure of nonpublic personal information

    a. Required, or one of the lawful or appropriate methods to enforce the rights of the institution or other persons engaged in carrying out the transaction or providing the product or service, or (§ 216.14(b)(1)) Yes No

    b. Required, or a usual, appropriate, or acceptable method under section 216.14(b)(2), to

        i. Carry out the transaction or the product or service business of which the transaction is a part, including recording, servicing, or maintaining the consumer's account in the ordinary course of business, (§ 216.14(b)(2)(i)) Yes No

        ii. Administer or service benefits or claims, (§ 216.14(b)(2)(ii)) Yes No

        iii. Confirm or provide a 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, (§ 216.14(b)(2)(iii)) Yes No

        iv. Accrue or recognize incentives or bonuses, (§ 216.14(b)(2)(iv)) Yes No

        v. Underwrite insurance or provide for reinsurance or for certain other purposes related to a consumer's insurance, or (§ 216.14(b)(2)(v)) Yes No

        vi. In connection with one of the following:

            (1) The authorization, settlement, billing, processing, clearing, transferring, reconciling, or collection of amounts charged, debited, or otherwise paid by using a debit, credit, or other payment card, check, or account number, or by other payment means (§ 216.14(b)(2)(vi)(A)) Yes No

            (2) The transfer of receivables, accounts, or interests therein (§ 216.4(b)(2)(vi)(B)) Yes No

            (3) The audit of debit, credit, or other payment information (§ 216.14(b)(2)(vi)(C)) Yes No

Other Exceptions to Notice and Opt-Out Requirements

50. If the institution discloses nonpublic personal information to nonaffiliated third parties, do certain requirements—for initial notice in section 216.4(a)(2); opt-out in sections 216.7 and 10; revised notice in section 216.8; and service providers and joint marketers in section 216.13—not apply because the institution makes the disclosure

    a. With the consent or at the direction of the consumer (§ 216.15(a)(1)) Yes No

    b. i. To protect the confidentiality or security of records (§ 216.15(a)(2)(i)) Yes No

        ii. To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability (§ 216.15(a)(2)(ii)) Yes No

        iii. For required institutional risk control or for resolving consumer disputes or inquiries (§ 216.15(a)(2)(iii)) Yes No

        iv. To persons holding a legal or beneficial interest relating to the consumer (§ 216.15(a)(2)(iv)) Yes No

        v. To persons acting in a fiduciary or representative capacity on behalf of the consumer (§ 216.15(a)(2)(v)) Yes No

    c. To insurance rate advisory organizations, guaranty funds or agencies, agencies rating the institution, persons assessing compliance, and the institution's attorneys, accountants, and auditors (§ 216.15(a)(3)) Yes No

d. In compliance with the Right to Financial Privacy Act, or to law enforcement agencies (§ 216.15(a)(4)) Yes No

e. To a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency (§ 216.15(a)(5)) Yes No

f. 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 only consumers of such business or unit (§ 216.15(a)(6)) Yes No

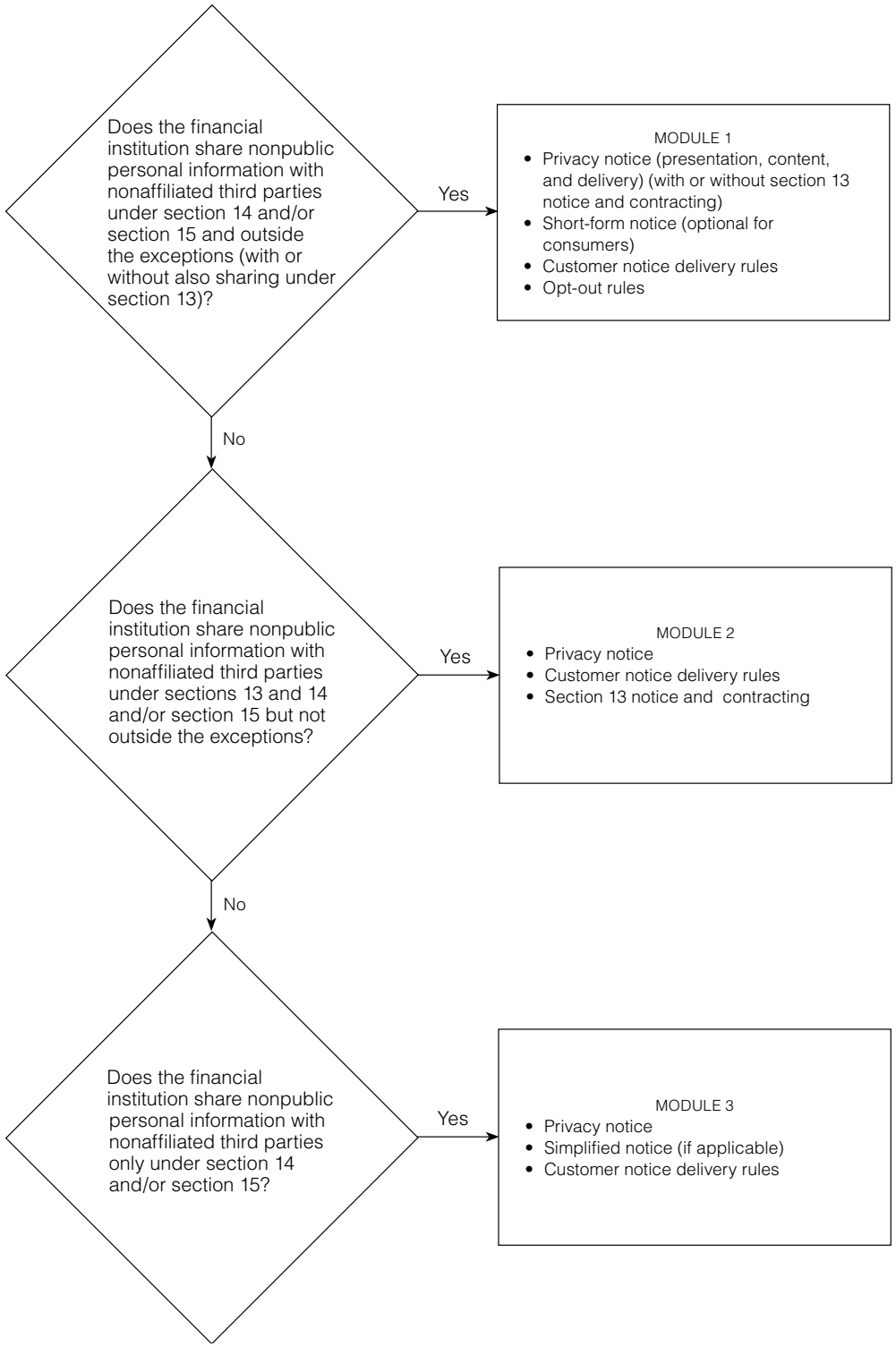
g. To comply with federal, state, or local laws, rules, or legal requirements (§ 216.15(a)(7)(i)) Yes No

h. To comply with a properly authorized civil, criminal, or regulatory investigation, or a subpoena or summons by federal, state, or local authorities (§ 216.15(a)(7)(ii)) Yes No

i. To respond to judicial process or government regulatory authorities having jurisdiction over the institution for examination, compliance, or other purposes as authorized by law (§ 216.15(a)(7)(iii)) Yes No

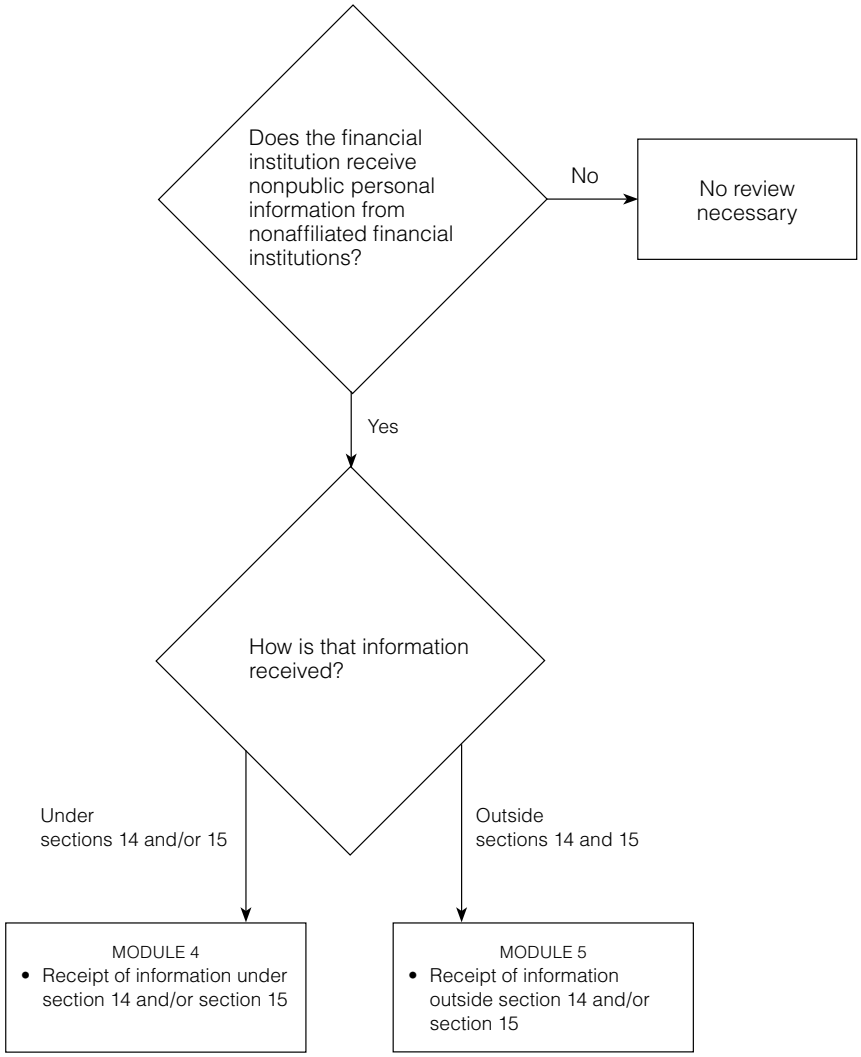
Note: The regulation gives the following as an example of the exception described in part a of this question: ''A consumer may specifically consent to disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to [the institution] for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.''

Appendix A. Decision Tree: Privacy Notices and Opt-Out Provisions



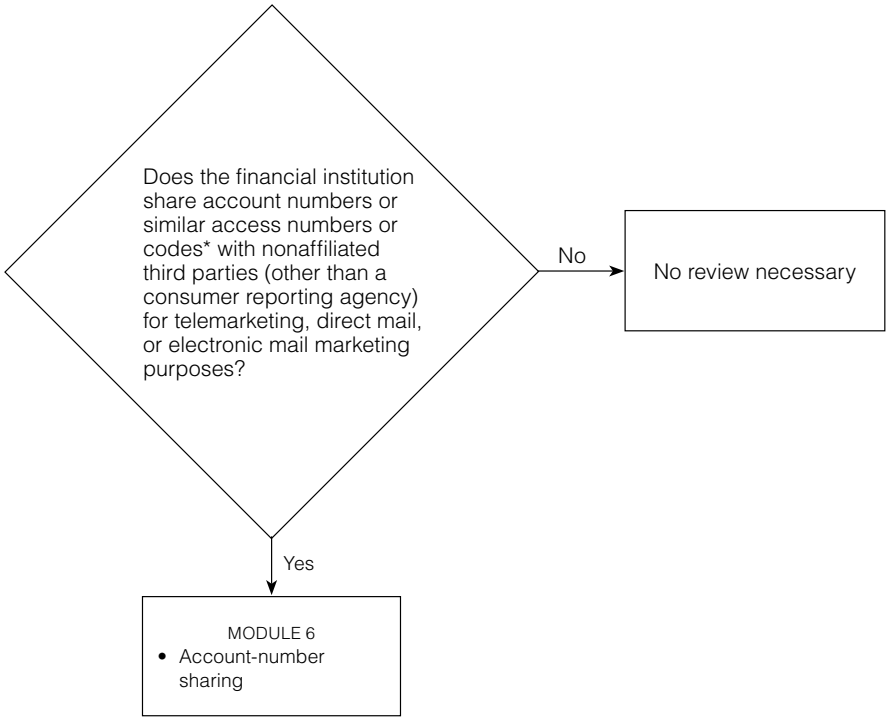
Appendix B. Decision Tree: Reuse and Redisclosure of Nonpublic Personal Information Received from Nonaffiliated Financial Institutions

(Sections 11(a) and 11(b))



Appendix C. Decision Tree: Account-Number Sharing

(Section 12)



* Including encrypted account numbers—but not the decryption key.