Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)

Introduction

Title V, Subtitle A of the Gramm-Leach-Bliley Act ("GLBA")[1] governs the treatment of nonpublic personal information about consumers by financial institutions. Section 502 of the Subtitle, subject to certain exceptions, prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties, unless (i) the institution satisfies various notice and opt-out requirements, and (ii) the consumer has not elected to opt out of the disclosure. Section 503 requires the institution to provide notice of its privacy policies and practices to its customers. Section 504 authorizes the issuance of regulations to implement these provisions.

In 2000, the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), the National Credit Union Administration ("NCUA"), the Office of the Comptroller of the Currency ("OCC"), and the former Office of Thrift Supervision ("OTS"), published regulations implementing provisions of the GLBA governing the treatment of nonpublic personal information about consumers by financial institutions.[2]

Title X of the Dodd-Frank Act Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act")[3] granted rulemaking authority for most provisions of Subtitle A of Title V of the GLBA to the Consumer Financial Protection Bureau ("CFPB") with respect to financial institutions and other entities subject to the CFPB's jurisdiction, except securities and futures-related companies and certain motor vehicle dealers. The Dodd-Frank Act also granted authority to the CFPB to examine and enforce compliance with these statutory provisions and their implementing regulations with respect to entities under CFPB jurisdiction.[4] In December 2011 the CFPB recodified in Regulation P, 12 CFR Part 1016, the implementing regulations that were previously issued by the Board, the FDIC, the Federal Trade Commission ("FTC"), the NCUA, the OCC, and the former OTS.[5]

The regulation establishes rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information, as summarized below.

- A financial institution must provide notice of its privacy policies and practices, and allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions in sections 13, 14, or 15 of the regulation. If the financial institution provides the consumer's nonpublic personal information to a nonaffiliated third party under the exception in section 13, it must provide notice of its privacy policies and practices to the consumer. Under the exception in section 13, the financial institution must also enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to perform services for the institution or functions on the institution's behalf, including use under an exception in sections 14 or 15 in the ordinary course of business to carry out those services or functions. If the financial institution complies with these requirements, it is not required to provide an opt out notice.
- Regardless of whether a financial institution shares nonpublic personal information, the institution must provide notice of its privacy policies and practices to its customers.
- A financial institution generally may not disclose consumer account numbers to any nonaffiliated third party for marketing purposes.
- A financial institution must follow redisclosure and reuse limitations on any nonpublic personal information it receives from a nonaffiliated financial institution.

In general, the privacy notice must describe a financial institution's policies and practices with respect to collecting and disclosing nonpublic personal information about a consumer to both affiliated and nonaffiliated third parties. Also, the notice must provide a consumer a reasonable opportunity to direct the institution generally not to share nonpublic personal information about the consumer (that is, to "opt out") with nonaffiliated third parties other than as permitted by exceptions under the regulation (for example, sharing for everyday business purposes, such as processing transactions and maintaining customers' accounts, and in response to properly executed governmental requests). The privacy notice must also provide, where applicable under the Fair Credit Reporting Act ("FCRA"), a notice and an opportunity for a consumer to opt out of certain information sharing among affiliates.

[1] 15 U.S.C. Sections6801-6809.

[2] The NCUA published its final rule in the *Federal Register* on May 18, 2000 (65 FR 31722). The Board, the FDIC, the OCC, and the former OTS jointly published their final rules on June 1, 2000 (65 FR 35162).

[3] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, Title X, 124 Stat. 1983 (2010).

[4] Dodd-Frank Act Sections1002(12)(J), 1024(b)-(c), and 1025(b)-(c); 12 U.S.C. Sections5481(12)(J), 5514(b)-(c), and 5515(b)-(c). Section 1002(12)(J) of the Dodd-Frank Act, however, excluded financial institutions' information security safeguards under GLBA section 501(b) from the CFPB's rulemaking, examination, and enforcement authority.

[5] 76 FR 79025 (Dec. 21, 2011). Pursuant to GLBA, the FTC retains rulemaking authority over any financial institution that is a person described in 12 U.S.C. Section5519 (with certain statutory exceptions, the FTC generally retains rulemaking authority for motor vehicle dealers predominantly engaged in the sale and servicing of motor vehicles, the leasing and servicing of motor vehicles, or both).

Section 728 of the Financial Services Regulatory Relief Act of 2006 required the four federal banking agencies (the Board, the FDIC, the OCC, and the former OTS) and four additional federal regulatory agencies (the Commodity Futures Trading Commission ("CFTC"), the FTC, the NCUA, and the Securities and Exchange Commission ("SEC")) to develop a model privacy form that financial institutions may rely on as a safe harbor to provide disclosures under the privacy rules.

On December 1, 2009, the eight federal agencies jointly released a voluntary model privacy form designed to make it easier for consumers to understand how financial institutions collect and share nonpublic personal information.[6] The final rule adopting the model privacy form was effective on December 31, 2009.

On October 28, 2014, the CFPB published a final rule amending the requirements regarding financial institutions' provision of their annual disclosures of privacy policies and practices to customers by creating an alternative delivery method that financial institutions can use under certain circumstances.[7] The amendment was effective immediately upon publication. The alternative delivery method allows a financial institution to provide an annual privacy notice by posting the annual notice on its web site, if the financial institution meets certain conditions.

Definitions and Key Concepts

In discussing the duties and limitations imposed by the regulation, a number of key concepts are used. These concepts include "financial institution"; "nonpublic personal information"; "nonaffiliated third party"; the "opt out" right and the exceptions to that right; and "consumer" and "customer." Each concept is briefly discussed below. A more complete explanation of each appears in the regulation.

Financial Institution: A "financial institution" is any institution the business of which 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.[8]

Nonpublic personal information: "Nonpublic personal information" generally is any information that is not publicly available and 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; or
- a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

Information is publicly available if an institution has a reasonable basis to believe that the information is lawfully made available to the general public from government records, widely distributed media, or legally required disclosures to the general public. Examples include information in a telephone book or a publicly recorded document, such as a mortgage or security interest filing.

Nonpublic personal information may include individual items of information as well as lists of information. For example, nonpublic personal information may include names, addresses, phone numbers, social security numbers, income, credit score, and information obtained through Internet collection devices (*i.e.*, cookies).

There are special rules regarding lists. Publicly available information would be treated as nonpublic if it were included on a list of consumers derived from nonpublic personal information. For example, a list of the names and addresses of a financial institution's depositors would be nonpublic personal information even though the same names and addresses might be published in local telephone directories, because the list is derived from the fact that a person has a deposit account with an institution, which is not publicly available information.

However, if the financial institution has a reasonable basis to believe 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 from public records would be considered publicly available information. The institution could provide a list of such customers, and include on that list any other publicly available information it has about those customers without having to provide notice or opt 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.

6 74 FR 62890.
7 79 FR 64057.
8 Certain functionally regulated subsidiaries, such as brokers, dealers, and investment advisers, are subject to GLBA implementing regulations issued by the SEC. Other functionally regulated subsidiaries, such as futures commission merchants, commodity trading advisors, commodity pool operators, and introducing brokers in commodities, are subject to GLBA implementing regulations issued by the CFTC. Insurance entities may be subject to privacy regulations issued by their respective state insurance authorities.

Opt Out Right and Exceptions:

The Right—Consumers must be given the right to "opt out" of, or prevent, a financial institution from disclosing nonpublic personal information about them to a nonaffiliated third party unless an exception to that right applies. The exceptions are detailed in sections 13, 14, and 15 of the regulation and described below.

As part of the opt out right, consumers must be given a reasonable opportunity and a reasonable means to opt 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, it would be reasonable if the financial institution allows 30 days from the date of mailing a notice or 30 days after customer acknowledgement of an electronic notice for an opt out direction to be returned. What constitutes a reasonable means to opt out may include check-off boxes, a reply form, or a toll-free telephone number. It is not reasonable to require a consumer to write his or her own letter as the only means to opt out.

The Exceptions

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

- Section 13: 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 an initial notice of these arrangements and by contract prohibits the third party from disclosing or using the information for other than the specified purposes. 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 disclosure and confidentiality requirements of section 13.
- Section 14: 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, administration of a rewards program, or provision of an account statement.
- Section 15: 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.

Consumer and Customer:

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

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

A **"financial service"** includes, among other things, a financial institution's evaluation 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.

Consumers who are not customers are entitled to an initial privacy and opt out notice before the financial institution shares nonpublic personal information with nonaffiliated third parties outside of the exceptions in sections 13, 14, and 15. Consumers who are not customers are entitled to an initial privacy notice before the financial institution shares nonpublic personal information with a nonaffiliated third party under the exception in section 13. Under the exception in section 13, the financial institution must also enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to perform services for the institution or functions on the institution's behalf, including use under an exception in sections 14 or 15 in the ordinary course of business to carry out those services or functions. If a financial institution complies with these requirements, it is not required to provide an opt out notice.

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; or

- obtains financial, investment, or economic advisory services for a fee.

Customers are entitled to initial and annual privacy notices regardless of the information disclosure practices of their financial institution.

There is a special rule for loans. When a financial institution sells the servicing rights to a loan to another financial institution, the customer relationship transfers with the servicing rights. However, any information on the borrower retained by the institution that sells the servicing rights 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 where the person has no account, the individual will be 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 where the individual has no account, even repeatedly, the individual will be a consumer, but not a customer of that institution.

Financial Institution Duties

The regulation establishes specific duties and limitations for a financial institution based on its activities. Financial institutions that intend to disclose nonpublic personal information outside the exceptions in sections 13, 14, and 15 will have to provide opt out rights to their customers and to consumers who are not customers. All financial institutions have an obligation to provide an initial and annual notice of their privacy policies and practices to their customers and to provide an initial notice to consumers who are not customers before disclosing nonpublic personal information to a nonaffiliated third party other than under sections 14 and 15. All financial 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 brief summary of financial institution duties and limitations appears below. A more complete explanation of each appears in the regulation.

Notice and Opt Out Duties to Consumers:

Before a financial institution discloses nonpublic personal information about any of its consumers to a nonaffiliated third party, and an exception in section 14 or 15 does not apply, then the financial institution must provide to the consumer:

- an initial notice of its privacy policies and practices;
- an opt out notice (including, among other things, a reasonable means to opt out); and
- a reasonable opportunity, before the financial institution discloses the information to the nonaffiliated third party, to opt out.

Before a financial institution discloses nonpublic personal information about a consumer to a nonaffiliated third party under the exception in section 13, the financial institution must provide to the consumer an initial notice of its privacy policies and practices. Under the exception in section 13, the financial institution must also enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to perform services for the institution or functions on the institution's behalf, including use under an exception in sections 14 or 15 in the ordinary course of business to carry out those services or functions. If a financial institution complies with these requirements, it is not required to provide an opt out notice.

The financial institution may not disclose any nonpublic personal information to nonaffiliated third parties except under the enumerated exceptions unless these notices have been provided and the consumer has not opted out (where applicable). Additionally, the institution must provide a revised notice before the financial institution begins to share a new category of nonpublic personal information or shares information with a new category of nonaffiliated third party 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 in sections 14 and 15. A financial institution that discloses nonpublic personal information about a consumer to a nonaffiliated third party under the exception in section 13 must provide an initial notice. Under the exception in section 13, the financial institution must also enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to perform services for the institution or functions on the institution's behalf, including use under an exception in sections 14 or 15 in the ordinary course of business to carry out those services or functions. If these requirements are met, the financial institution is not required to provide an opt out notice.

Notice Duties to Customers:

In addition to the duties described above, there are several duties unique to customers. In particular, regardless of whether the institution discloses or intends to disclose nonpublic personal information, a financial institution must provide notice to its customers of its privacy policies and practices at various times.

- A financial institution must provide an initial notice of its privacy policies and practices to each customer, not later

than the time a customer relationship is established. Section 4(e) of the regulation describes the exceptional cases in which delivery of the notice is allowed subsequent to the establishment of the customer relationship.

- A financial institution must provide an annual notice at least once in any period of 12 consecutive months during the continuation of the customer relationship.
- Generally, new privacy notices are not required for each new product or service. However, a financial institution 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.
- When a financial 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, the institution has the option of providing a simplified notice.

Requirements for Notices

Clear and Conspicuous. Privacy notices must be clear and conspicuous, meaning they must be reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. The regulation does not prescribe specific methods for making a notice clear and conspicuous, but does provide examples of ways in which to achieve the standard, such as the use of short explanatory sentences or bullet lists, and the use of plain-language headings and easily readable typeface and type size. 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 its consumers, (2) mail a printed copy of the notice to a consumer's last known address, or (3) for the consumer who conducts transactions electronically, post the notice on the institution's web site and require the consumer to acknowledge receipt of the notice as a necessary step to 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.

A financial institution may use an alternative delivery method for providing annual privacy notices to customers through posting the annual notices on their web sites if: (1) no opt out rights are triggered by the financial institution's information sharing practices under GLBA or under FCRA section 603, and opt out notices required by FCRA section 624 and Subpart C of Regulation V have previously been provided, if applicable, or the annual privacy notice is not the only notice provided to satisfy those requirements; (2) certain information included in the annual privacy notice has not changed since the previous notice; and (3) the financial institution uses the model form provided in the regulation as its annual privacy notice. In order to use this alternative delivery method, an institution must: (1) insert a clear and conspicuous statement at least once per year on an account statement, coupon book, or a notice or disclosure the institution issues under any provision of law that informs customers that the annual privacy notice is available on the institution's web site, that the institution will mail the notice to customers who request it by calling a specific telephone number, and that the notice has not changed; (2) continuously post the current privacy notice in a clear and conspicuous manner on a page on its web site, on which the only content is the privacy notice, without requiring the customer to provide any information such as a login name or password or agree to any conditions to access the web site; and (3) mail its current privacy notice to those customers who request it by telephone within ten calendar days of the request.

Notice Content. A privacy notice must contain specific disclosures. However, a financial institution may provide to consumers who are not also customers a "short form" initial notice together with an opt out notice stating that the institution's privacy notice is available upon request and explaining a reasonable means for the consumer to obtain it. The following is a list of disclosures regarding nonpublic personal information that institutions must provide in their privacy notices, as applicable:

1. categories of information collected;
2. categories of information disclosed;
3. categories of affiliates and nonaffiliated third parties to whom the institution may disclose information;
4. policies and practices with respect to the treatment of former customers' information;
5. categories of information disclosed to nonaffiliated third parties that perform services for the institution or functions on the institution's behalf and categories of third parties with whom the institution has contracted (Section 13);
6. an explanation of the opt out right and methods for opting out;
7. any opt out notices that the institution must provide under the FCRA with respect to affiliate information sharing;

8. policies and practices for protecting the security and confidentiality of information; and
9. a statement that the institution makes disclosures to other nonaffiliated third parties for everyday business purposes or as permitted by law (Sections 14 and 15).

Model Privacy Form. The Appendix to the regulation contains the model privacy form. A financial institution can use the model form to obtain a "safe harbor" for compliance with the content requirements for notifying consumers of its information-sharing practices and their right to opt out of certain sharing practices. To obtain the safe harbor, the institution must provide a model form in accordance with the instructions set forth in the Appendix of the regulation. Additionally, institutions using the alternative delivery method for providing annual privacy notices to customers must use the model form.

Limitations on Disclosure of Account Numbers (section 12):

A financial institution must not disclose an account number or similar form of access number or access code for a credit card, deposit, 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.

The disclosure of encrypted account numbers without an accompanying means of decryption, however, is not subject to this prohibition. The regulation also expressly allows disclosures by a financial institution to its agent to market the institution's own products or services (although the financial institution must not authorize the agent to directly initiate charges to the customer's account). The regulation also does not bar a financial institution from disclosing account numbers to participants in private-label or affinity card programs, if the participants are identified to the customer when the customer enters the program.

Redisclosure and Reuse Limitations on Nonpublic Personal Information Received (section 11):

If a financial institution receives nonpublic personal information from a nonaffiliated financial institution, its disclosure and use of the 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 can do so; and
  - Disclosing and using the information pursuant to 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 received other than 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 can do so; and
  - 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 in accordance with the privacy policy of the financial institution that provided the list, subject to any opt out election or revocation by the consumers on the list, and in accordance with appropriate exceptions under sections 14 and 15.

Other Matters

Fair Credit Reporting Act

The regulation does not modify, limit, or supersede the operation of the FCRA.

State Law

The regulation 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 interpretation is consistent with the regulation if the protection it affords any consumer is greater than the protection provided under the regulation, as determined by the CFPB, on its own motion or upon the petition of any interested party, after consultation with the agency or authority with jurisdiction under section 505(a) of the GLBA over either the person who initiated the complaint or that is the subject of the complaint.

Guidelines Regarding Protecting Customer Information

The regulation 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, but instead 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 four federal banking agencies published guidelines, pursuant to section 501(b) of the GLBA, that address 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 information security.

Examination Objectives

1. To assess the quality of a financial institution's compliance management policies, procedures, and internal controls for implementing the regulation, 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 policies, procedures, and internal controls for monitoring the institution's compliance with the regulation.
3. To determine a financial institution's compliance with the regulation, 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; and

     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, procedures, or internal controls are deficient.

Examination Procedures[9]

A. Through discussions with management and review of available information, identify the institution's information sharing practices (and changes to those practices) with affiliates and nonaffiliated third parties; how it 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, procedures, and internal controls, including those to:
   - Process requests for nonpublic personal information, including requests for aggregated information;
   - Deliver notices to consumers;
   - Manage consumer opt out directions (*e.g.*, designating 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; and

     prevent the unlawful disclosure of account numbers;
3. Information sharing agreements between the institution and affiliates and service agreements or contracts between the institution and nonaffiliated third parties either 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 in obtaining a financial product or service (e.g., 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 information 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 those received electronically;
8. Records that reflect the bank's categorization of its information sharing practices under Sections 13, 14, 15, and outside of these exceptions;

[9] These reflect the interagency examination procedures in their entirety.

9. Results of a 501(b) inspection (used to determine the accuracy of the institution's privacy disclosures regarding information security).

B. Use the information gathered from step A to work through the "Privacy Notice and Opt Out Decision Tree" (Attachment A). Identify which module(s) of procedures is (are) applicable.

C. Use the information gathered from step A to work through the Redisclosure and Reuse and Account Number Sharing Decision Trees, as necessary (Attachments B and C). Identify which module is applicable.

D. Determine the adequacy of the financial institution's policies, procedures, and internal controls to ensure compliance with the regulation as applicable. Consider the following:

1. Sufficiency of internal policies, procedures, and internal controls, including review of new products and services and controls over servicing arrangements and marketing arrangements;
2. Effectiveness of management information systems, including the use of technology for monitoring, exception reports, and standardization of forms and procedures;
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; and
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 of the exceptions) and any weaknesses found within the compliance management program. Keep in mind any outstanding deficiencies identified in the audit for follow-up when completing the modules.

F. Based on the results of the foregoing initial procedures and discussions with management, determine which procedures if any should be completed in the applicable module, focusing on areas of particular risk. The selection of procedures to be employed depends upon the adequacy of the institution's compliance management system and level of risk identified. Each module contains a series of general instructions to verify compliance, cross-referenced to cites within the regulation. Additionally, there are cross-references to a more comprehensive checklist, which the examiner may use if needed to evaluate compliance in more detail.

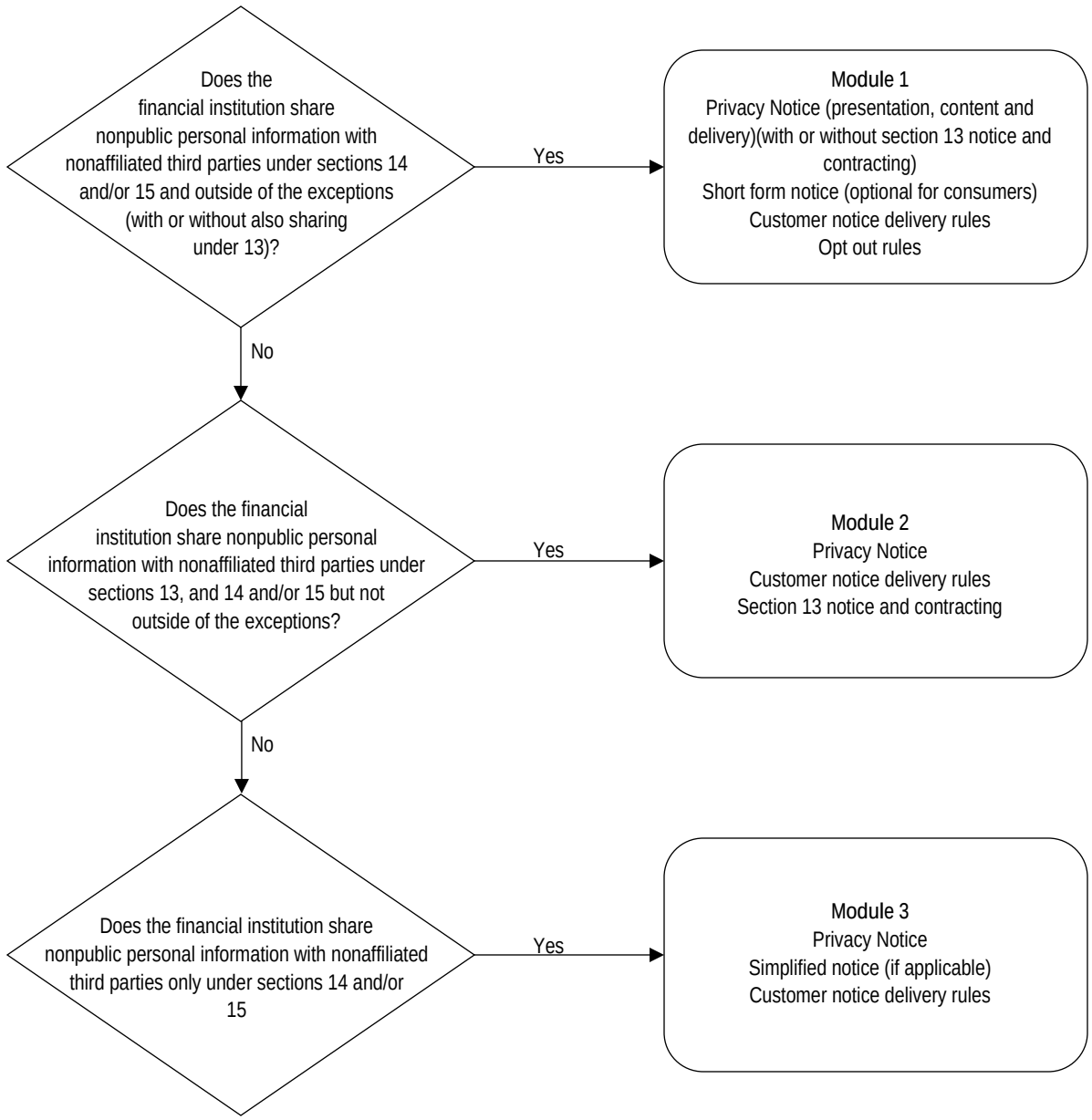
G. Evaluate any additional information or documentation discovered during the course of the examination according to these procedures. Note that this may reveal new or different sharing practices necessitating reapplication of the Decision Trees and completion of additional or different modules.

H. Formulate conclusions.

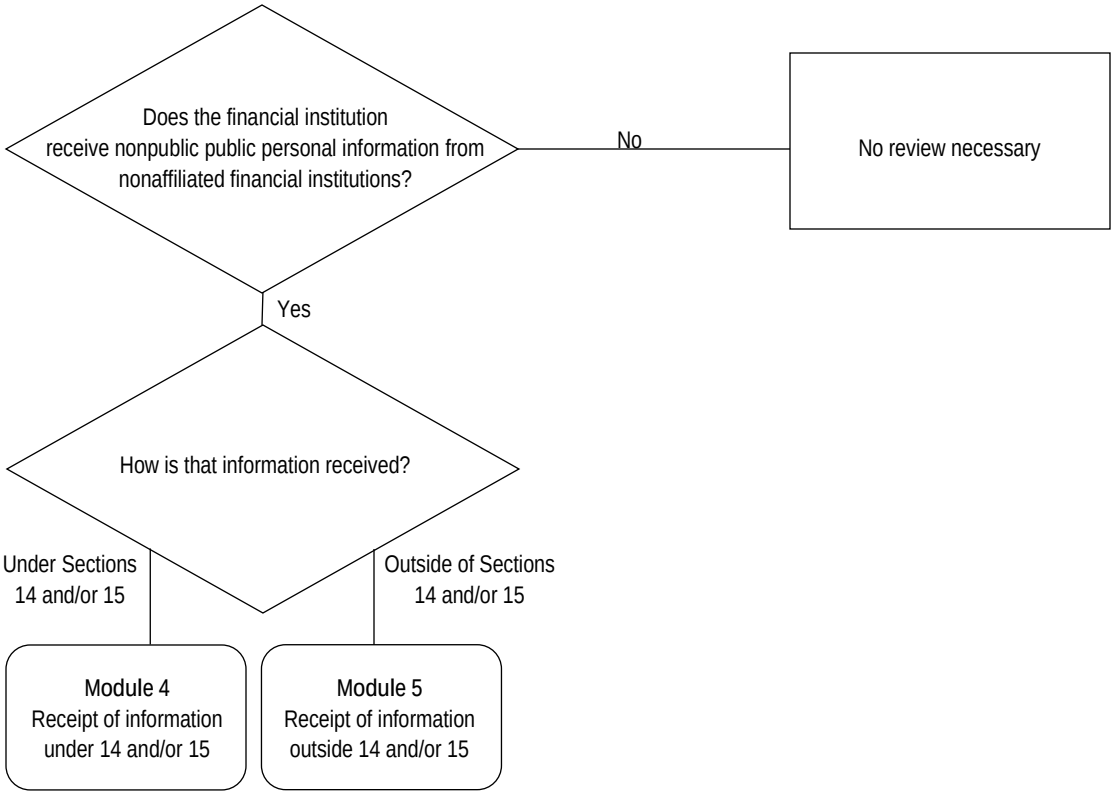
Summarize all findings.

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

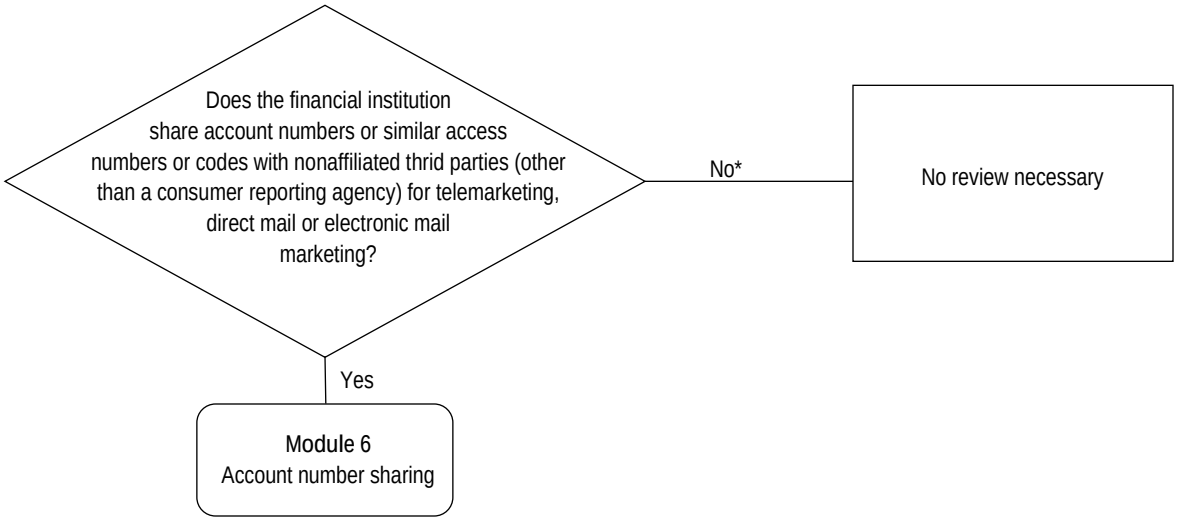
Privacy Notice and Opt Out Decision Tree



Redisclosure and Reuse of Nonpublic Personal Information Received from Nonaffiliated Financial Institutions Decision Tree (Sections 11(a) and 11(b))



Account Number Sharing Decision Tree (Section 12)



*This may include sharing of encrypted account numbers but not the decryption key.

Module 1

Sharing nonpublic personal information with nonaffiliated third parties under Sections 14 and/or 15 and outside of 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 regulation.

A. Disclosure of Nonpublic Personal Information

1. Select a sample of third party relationships with nonaffiliated third parties and obtain a sample of information shared between the institution and the third party both inside and outside of 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. Perform the following comparisons to evaluate the financial institution's compliance with disclosure limitations.
   a. Compare the categories of information shared and with whom the information was shared to those stated in the privacy notice and verify that what the institution tells consumers (both customers and those who are not customers) in its notices about its policies and practices in this regard and what the institution actually does are consistent. (Sections 6,10)
   b. Compare the information shared to 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 (Section 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 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 (Section 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 (Sections 3(b), 4(a), 5(a)(1), 8(a)(1));
   b. Accurately reflect the institution's policies and practices. (Sections 4(a), 5(a)(1), 8(a)(1))
      NOTE: this includes policies and practices disclosed in the notices that exceed regulatory requirements; and
   c. Include, and adequately describe, all required items of information and contain examples as applicable (Section 6). Note that if the institution shares under nonpublic personal information under Section 13 the notice provisions for that section shall also apply.
   d. If the model privacy form is used, determine that it reflects the institution's policies and practices. For institutions seeking a safe harbor for compliance with the content requirements of the regulation, verify that the notice has the proper content and is in the proper format as specified in the Appendix A of the regulation.
2. Through discussions with management, review of the institution's policies, procedures, and internal controls and a sample of electronic or written consumer records where available, determine if the institution has adequate policies, procedures, and internal controls in place to provide notices to consumers, as appropriate. Assess the following:

   Timeliness of delivery (Sections 4(a), 7(c), 8(a)); and
   a. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the consumer agrees; or as a necessary step of a transaction) (Section 9).
   b. For customers only, review the timeliness of delivery (Sections 4(d), 4(e), 5(a)), means of delivery of annual notice (Section 9(c)), and accessibility of or ability to retain the notice (Section 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 (Sections 3(b) and 7(a)(1));
   b. Accurately explain the right to opt out (Section 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) (Section 7(a)(1)); and
   d. Describe how the institution treats joint relationships, as applicable (Section 7(d)).
2. Through discussions with management, review of the institution's policies, procedures, and internal controls

and a sample of electronic or written consumer records where available, determine if the institution has adequate policies, procedures, and internal controls in place to provide notices to consumers, as appropriate. Assess the following:

a. Timeliness of delivery (Section 10(a)(1));

b. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the consumer agrees; or as a necessary step of a transaction) (Section 9).

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

d. Adequacy of procedures to implement and track the status of a consumer's (customers and those who are not customers) opt out direction, including those of former customers (Section 7(e), (f), (g)).

D. Checklist Cross References—Module1

Regulation Section	**Subject**	**Checklist Questions**
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, 41
4(a, c, d, e); 5; and 9(c, e)	Customer notice delivery rules	1, 3-7, 37, 39
13	Section 13 notice and contracting rules (as applicable)	12, 48
6(d)	Short form notice rules (optional for consumers only)	15-17
7; 8; and 10	Opt out rules	19-34, 42-44
14, 15	Exceptions	49- 50

Module 2

Sharing nonpublic personal information with nonaffiliated third parties under Sections 13, and 14 and/or 15 but not outside of these exceptions

A. Disclosure of Nonpublic Personal Information

1. Select a sample of third party relationships with nonaffiliated third parties and obtain a sample of information 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. Perform the following comparisons to evaluate the financial institution's compliance with disclosure limitations.
   a. Compare the information shared and with whom the information was shared to ensure that the institution accurately categorized its information sharing practices and is not sharing nonpublic personal information outside the exceptions. (Sections 13, 14, 15)
   b. Compare the categories of information shared and with whom the information was shared to those stated in the privacy notice and verify that what the institution tells consumers in its notices about its policies and practices in this regard and what the institution actually does are consistent. (Sections 10, 6)
   c. If the model privacy form is used, determine that it reflects the institution's policies and practices. For institutions seeking a safe harbor for compliance with the content requirements of the regulation, verify that the notice has the proper content and is in the proper format as specified in the Appendix of the regulation.
2. Review contracts with nonaffiliated third parties that perform services for the financial institution 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 (Section 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 (Sections 3(b), 4(a), 5(a)(1));
   b. Accurately reflect the institution's policies and practices (Sections4(a), 5(a)(1)). Note, this includes policies and practices disclosed in the notices that exceed regulatory requirements; and
   c. Include, and adequately describe, all required items of information and contain examples as applicable. (Sections 6, 13)
2. Through discussions with management, review of the institution's policies, procedures, and internal controls and a sample of electronic or written consumer records where available, determine if the institution has adequate policies, procedures, and internal controls in place to provide notices to consumers, as appropriate. Assess the following:
   a. Timeliness of delivery (Section 4(a)); and
   b. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the consumer agrees; as a necessary step of a transaction; or pursuant to the alternative delivery method) (Section9).
   c. For customers only, review the timeliness of delivery (Sections 4(d), 4(e), and 5(a)), means of delivery of annual notice Section 9(c)), and accessibility of or ability to retain the notice (Section 9(e)).

C. Checklist Cross References—Module 2

Regulation Section	Subject	Checklist Questions
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, 41
4(a, c, d, e); 5; and 9(c, e)	Customer notice delivery rules	1, 3-7, 37, 39
13	Section 13 notice and contracting rules	12, 48
14, 15	Exceptions	49-51

Module 3

Sharing nonpublic personal information with nonaffiliated third parties only under Sections 14 and/or 15.

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 obtain a sample of information shared between the financial institution and the third party.
      a. Compare the information shared and with whom the information was 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 that the institution may use. Note that the institution may only use the simplified notice when it does not also share nonpublic personal information with affiliates outside of Section 14 and 15 exceptions. Determine whether or not these notices:
      a. Are clear and conspicuous (Sections 3(b), 4(a), 5(a)(1));
      b. Accurately reflect the institution's policies and practices (Sections 4(a), 5(a)(1)). Note, this includes practices disclosed in the notices that exceed regulatory requirements; and
      c. Include, and adequately describe, all required items of information (Section 6).
      d. If the model privacy form is used, determine that it reflects the institution's policies and practices. For institutions seeking a safe harbor for compliance with the content requirements of the regulation, verify that the notice has the proper content and is in the proper format as specified in the Appendix of the regulation.
   2. Through discussions with management, review of the institution's policies, procedures, and internal controls and a sample of electronic or written customer records where available, determine if the institution has adequate policies, procedures, and internal controls in place to provide notices to customers, as appropriate. Assess the following:
      a. Timeliness of delivery (Sections 4(a), 4(d), 4(e), 5(a)); and
      b. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the customer agrees; as a necessary step of a transaction; or pursuant to the alternative delivery method) (Section 9) and accessibility of or ability to retain the notice (Section 9(e)).

C. Checklist Cross References—Module 3

Regulation Section	Subject	Checklist Questions
4(a, d, e); 5; and 9	Customer notice delivery process	1, 3,-7, 35-41
6	Customer notice content and presentation	8-11, 14, 18
6(c)(5);	Simplified notice content (optional)	13
14, 15	Exceptions	49-51

Module 4

Redisclosure and Reuseof nonpublic personal information received from a nonaffiliated financial institution under Sections 14 and/or 15.

A. Through discussions with management and review of the institution's policies, procedures, and internal controls, determine whether the institution has adequate policies, procedures, and internal controls to prevent the unlawful redisclosure and reuse of the information where the institution is the recipient of nonpublic personal information (Section 11(a)).

B. Select a sample of information received from nonaffiliated financial institutions, to evaluate the financial institution's compliance with redisclosure and reuse 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 in the step 2 below (Section 11(a)(1)(i) and (ii)).
   2. Verify that the institution only uses and shares the information pursuant to an exception in Sections 14 and 15 (Section 11(a)(1)(iii)).

C. Checklist Cross References—Module 4

Regulation Section	Subject	Checklist Questions
11(a)	Reuse and disclosure presentation	45
14, 15	Exceptions	49-51

Module 5

Redisclosure of nonpublic personal information received from a nonaffiliated financial institution outside of Sections 14 and 15.

A. Through discussions with management and review of the institution's policies, procedures, and internal controls, determine whether the institution has adequate policies, procedures, and internal controls to prevent the unlawful redisclosure of the information where the institution is the recipient of nonpublic personal information (Section 11(b)).

B. Select a sample of information received from nonaffiliated financial institutions and shared with others to evaluate the financial institution's compliance with 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 in the step 2 below (Section 11(b)(1)(i) and (ii)).
   2. If the institution shares information with entities other than those under step 1 above, verify that the institution's information sharing practices conform to those in the nonaffiliated financial institution's privacy notice (Section 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 (Sections 10, 11(b)(1)(iii)).

C. Checklist Cross References—Module 5

Regulation Section	Subject	Checklist Questions
11(b)	Redisclosure	46

Module 6

Account number sharing

A. If available, review a sample of telemarketer scripts used when making sales calls to determine whether the scripts indicate that the telemarketers have the account numbers of the institution's consumers (Section 12(a)).

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 perform 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 the accounts (Section 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 (Section 12(b)(2)).

D. Checklist Cross References—Module 6

Regulation Section	Subject	Checklist Questions

12	Account number sharing	47

References

Listed below are links to several Privacy resources, including the official examination procedures and the examination job-aid.

Regulations

FDIC Part 332: Privacy of Consumer Financial Information

FILs

FIL 01-106: Privacy of Consumer Financial Information

Job Aids

FDIC Staff Response to Questions Regarding the Privacy of Consumer Financial Information

Privacy of Consumer Financial Information - FDIC Part 332 Compliance Examination Job-Aid

Examination Checklist Subpart A	Yes	No
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 4 of the regulation? [Section 4(a)(1))] *NOTE: A financial institution establishes a customer relationship when it enters into a continuing relationship with a consumer. [Section 4(c)(1)] 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. [Section 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 Sections 14 or 15? [Section 4(a)(2)] *NOTE: no notice is required if nonpublic personal information is disclosed to nonaffiliated third parties only under an exception in Sections 14 and 15 and there is no customer relationship. [Section 4(b)])*		
3. Does the institution provide to existing customers, who obtain a revised 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? [Section 4(d)(1)]		
4. Does the institution provide initial notice after establishing a *customer relationship* only if:		
a. the customer relationship is not established at the customer's election; [Section 4(e)(1)(i)] or		
b. o do otherwise would substantially delay the customer's transaction (e.g. in the case of a telephone application), and the customer agrees to the subsequent delivery? [Section 4(e)(1)(ii)]		
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? [Section 4(e)]		
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? [Section 5(a)(1)and (2)] *NOTE: annual notices are not required for former customers. [Section 5(b)(1)and (2)]*		
7. Does the institution provide an annual privacy notice to each customer whose loan the institution owns the right to service? [Sections 5(c), 4(c)(2)]		
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; [Section 6(a)(1)]		
b. the categories of nonpublic personal information that the institution discloses; [Section 6(a)(2)]		
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 14 or Section 15; [Section 6(a)(3)]		

Examination Checklist Subpart A	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 14 or Section 15; [Section 6(a)(4)]		
e. if the institution discloses nonpublic personal information to a nonaffiliated third party under Section 13, and no exception under Section 14 or Section 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; [Section 6(a)(5)]		
f. an explanation of the opt out right, including the method(s) of opt out that the consumer can use at the time of the notice; [Section 6(a)(6)]		
g. any disclosures that the institution makes under FCRA Section 603(d)(2)(A)(iii); [Section 6(a)(7)]		
h. the institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; [Section 6(a)(8)] and		
i. a general statement – with no specific reference to the third parties – that the institution makes disclosures to other nonaffiliated third parties for everyday business purposes, such as (with the institution including all that are applicable) to process transactions, maintain accounts, respond to court orders and legal investigations, or report to credit bureaus, or as otherwise permitted by law? [Section 6(a)(9), (b)(1) and (2)] *NOTE: Institutions that provide a model privacy form in accordance with the instructions in the Appendix of the regulation will receive a safe harbor for compliance with the content requirements of the regulation.*		
9. Does the institution list the following categories of nonpublic personal information that it collects, as applicable:		
a. information from the consumer; [Section 6(c)(1)(i)]		
b. information about the consumer's transactions with the institution or its affiliates; [Section 6(c)(1)(ii)]		
c. information about the consumer's transactions with nonaffiliated third parties; [Section 6(c)(1)(iii)] and		
d. information from a consumer reporting agency? [Section 6(c)(1)(iv)]		
10. Does the institution list the following Section 6(c)(1) 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;		
b. information about the consumer's transactions with the institution or its affiliates;		
c. information about the consumer's transactions with nonaffiliated third parties; and		
d. information from a consumer reporting agency? [Section 6(c)(2)] *NOTE: examples are recommended under Section 6(c)(2(i)) although not under Section 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 the third parties in each category:		

Examination Checklist Subpart A	Yes	No
a. financial service providers; [Section 6(c)(3)(i)]		
b. non-financial companies; [Section 6(c)(3)(ii)] and		
c. others? [Section 6(c)(3)(iii)]		
12. Does the institution make the following disclosures regarding service providers and joint marketers to whom it discloses nonpublic personal information under Section 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 6 (*see* questions 8b and 10); [Section 6(c)(4)(i)] and		
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; [Section 6(c)(4)(ii)(A)] or		
c. that the third party is a financial institution with which the institution has a joint marketing agreement? [Section 6(c)(4)(ii)(B)]		
13. If the institution does not disclose nonpublic personal information, and does not reserve the right to do so, other than under exceptions in Section 14 and Section 15, does the institution provide a simplified privacy notice that contains at a minimum:		
a. a statement to this effect;		
b. the categories of nonpublic personal information it collects (same as paragraph (a)(1) of section 6);		
c. the policies and practices the institution uses to protect the confidentiality and security of nonpublic personal information (same as paragraph (a)(8) of section 6); and		
d. a general statement that the institution makes disclosures to other nonaffiliated third parties as permitted by law (same as paragraphs (a)(9) and (b) of section 6)? [Section 6(c)(5)] *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; [Section 6(c)(6)(i)] and		
b. whether security practices and policies are in place to ensure the confidentiality of the information in accordance with the institution's policy? [Section 6(c)(6)(ii)] *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? [Section 6(d)(1)]		
16. If the institution provides a short-form initial privacy notice according to Section 6(d)(1), does the short-form initial notice:		
a. conform to the definition of "clear and conspicuous"; [Section 6(d)(2)(i)]		
b. state that the institution's full privacy notice is available upon request; [Section 6(d)(2)(ii)] and		
c. explain a reasonable means by which the consumer may obtain the notice? [Section 6(d)(2)(iii)]		

Examination Checklist Subpart A	Yes	No
NOTE: the institution is not required to deliver the full privacy notice with the short-form initial notice. [Section 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; [Section 6(d)(4)(i)] or		
b. for the consumer who conducts business in person at the institution's office, having copies available to provide immediately by hand-delivery? [Section 6(d)(4)(ii)]		
18. If the institution, in its privacy policies and practices, reserves the right to disclose nonpublic personal information to nonaffiliated third parties in the future, does the privacy notice include, as applicable, the:		
a. categories of nonpublic personal information that the financial institution reserves the right to disclose in the future, but does not currently disclose; [Section 6(e)(1)] and		
b. categories of affiliates or nonaffiliated third parties to whom the financial institution reserves the right in the future to disclose, but to whom it does not currently disclose, nonpublic personal information? [Section 6(e)(2)]		
Opt Out Notice		
19. If the institution discloses nonpublic personal information about a consumer to a nonaffiliated third party, and the exceptions under Sections 13, 14, and 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? [Section 7(a)(1)		
20. Does the opt out notice state:		
a. that the institution discloses or reserves the right to disclose nonpublic personal information about the consumer to a nonaffiliated third party; [Section 7(a)(1)(i)]		
b. that the consumer has the right to opt out of that disclosure; [Section 7(a)(1)(ii)] and		
c. a reasonable means by which the consumer may opt out? [Section 7(a)(1)(iii)]		
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; [Section 7(a)(2)(i)(A)]		
b. all the categories of nonaffiliated third parties to whom the information is disclosed; [Section 7(a)(2)(i)(A)];		
c. that the consumer has the right to opt out of the disclosure of that information; [Section 7(a)(2)(i)(A)] and		
d. the financial products or services that the consumer obtains to which the opt out direction would apply? [Section 7(a)(2)(i)(B)]		
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; [Section 7(a)(2)(ii)(A)]		

Examination Checklist Subpart A	Yes	No
b. a reply form included with the opt out notice; [Section 7(a)(2)(ii)(B)]		
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; [Section 7(a)(2)(ii)(C)] or		
d. a toll-free telephone number? [Section 7(a)(2)(ii)(D)] *NOTE: the institution may require the consumer to use one specific means, as long as that means is reasonable for that consumer. [Section 7(a)(2)(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? [Section 7(c)]		
24. Does the institution provide an opt out notice, explaining how the institution will treat opt out directions by the joint consumers, to at least one party in a joint consumer relationship? [Section 7(d)(1)]		
25. Does the institution permit each of the joint consumers in a joint relationship to opt out? [Section 7(d)(2)]		
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; [Section 7(d)(2)(i)] or		
b. each joint consumer is permitted to opt out separately? [Section 7(d)(2)(ii)]		
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; [Section 7(d)(3)]		
b. the joint consumers to notify the institution in a single response; [Section 7(d)(5)(i)] and		
c. each joint consumer to opt out either for himself or herself, and/or for another joint consumer? [Section 7(d)(5)(ii)]		
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? [Section 7(d)(4)]		
29. Does the institution comply with a consumer's direction to opt out as soon as is reasonably practicable after receiving it? [Section 7(g)]		
30. Does the institution allow the consumer to opt out at any time? [Section 7(h)]		
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? [Section 7(i)(1)]		
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)? [Section 7(i)(2)]		
Revised Notices		
33. Except as permitted by Sections 13, 14, and 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:		

Examination Checklist Subpart A	Yes	No
a. the institution has provided the consumer with a clear and conspicuous revised notice that accurately describes the institution's privacy policies and practices; [Section 8(a)(1)]		
b. the institution has provided the consumer with a new opt out notice; [Section 8(a)(2)]		
c. the institution has given the consumer a reasonable opportunity to opt out of the disclosure, before disclosing any information; [Section 8(a)(3)] and		
d. the consumer has not opted out? [Section 8(a)(4)]		
34. Does the institution deliver a revised privacy notice when it:		
a. discloses a new category of nonpublic personal information to a nonaffiliated third party; [Section 8(b)(1)(i)]		
b. discloses nonpublic personal information to a new category of nonaffiliated third party; [Section 8(b)(1)(ii)] or		
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? [Section 8(b)(1)(iii)] *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. [Section 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 actual notice in writing or, if the consumer agrees, electronically? [Section 9(a)]		
36 Does the institution use a reasonable means for delivering the notices, such as:		
a. hand-delivery of a printed copy; [Section 9(b)(1)(i)]		
b. mailing a printed copy to the last known address of the consumer; [Section 9(b)(1)(ii)]		
c. for the consumer who conducts transactions electronically, clearly and conspicuously posting the notice on the institution's electronic site and requiring the consumer to acknowledge receipt as a necessary step to obtaining a financial product or service; [Section 9(b)(1)(iii)] or		
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? [Section 9(b)(1)(iv)] *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. [Section 9 (b)(2)(i) and (ii), and (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 such as:		
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; [Section 9(c)(1)(i)] or		
b. for the customer who has requested the institution refrain from sending any information about the		

Examination Checklist Subpart A	Yes	No
customer relationship, making copies of the current privacy notice available upon customer request? [Section 9(c)(1)(ii)]		
38. For annual notices only, if the institution uses the alternative delivery method does the institution meet the following conditions:		
a. the institution does not disclose the customer's nonpublic personal information to nonaffiliated third parties other than for purposes under sections 13, 14, and 15; [Section9(c)(2)(i)(A)]		
b. the institution does not include on its privacy notice an opt out under FCRA section 603(d)(2)(A)(iii); [Section9(c)(2)(i)(B)]		
c. the institution previously provided the customer the opt out notices required by FCRA section 624 and Subpart C of Regulation V, if applicable, or the privacy notice is not the only notice provided to satisfy those requirements; [Section9(c)(2)(i)(C)]		
d. the information that the institution is required to convey on its privacy notice pursuant to sections 6(a)(1)-(5), (8), and (9) has not changed since it provided the immediately previous privacy notice to the customer, other than to eliminate categories of information that it discloses or categories of third parties to which it discloses information; [Section9(c)(2)(i)(D)]		
e. the institution uses the model privacy form for its privacy notice; [Section9(c)(2)(i)(E)]		
f. the institution conveys in a clear and conspicuous manner not less than annually on an account statement, coupon book, or a notice or disclosure that it is required or expressly and specifically permitted to issue to the customer under any other provision of law that the privacy notice is available on its web site and will be mailed to the customer upon request by telephone, and the statement states that the privacy notice has not changed and includes a specific web address that takes the customer to the web site where the privacy notice is pasted and a telephone number for the customer to request that it be mailed; [Section9(c)(2)(ii)(A)]		
g. the institution posts its privacy notice continuously and in a clear and conspicuous manner on a page on its web site on which the only content is the privacy notice, without requiring the customer to provide any information such as a login name or password or agree to any conditions to access the web site; [Section9(c)(2)(ii)(B)] and		
h. the institution mails its current privacy notice to those customers who request it by telephone within ten calendar days of the request? [Section9(c)(2)(ii)(C)]		
39. For customers only, does the institution ensure that the initial, annual, and revised notices may be retained or obtained later by the customer in writing, or if the customer agrees, electronically? [Section 9(e)(1)]		
40. Does the institution use an appropriate means to ensure that notices may be retained or obtained later, such as:		
a. hand-delivery of a printed copy of the notice; [Section 9(e)(2)(i)]		
b. mailing a printed copy to the last known address of the customer; [Section 9(e)(2)(ii)] or		
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? [Section 9(e)(2)(iii)]		
41. Does the institution provide at least one initial, annual, and revised notice, as applicable, to joint consumers? [Section 9(g)]		

Examination Checklist Subpart B	Yes	No
Limits on Disclosure to Nonaffiliated Third Parties		
42. Does the institution refrain from disclosing any nonpublic personal information about a consumer to a nonaffiliated third party, other than as permitted under Sections 13, 14, and 15, unless:		
a. it has provided the consumer with an initial notice; [Section 10(a)(1)(i)]		
b. it has provided the consumer with an opt out notice; [Section 10(a)(1)(ii)]		
c. it has given the consumer a reasonable opportunity to opt out before the disclosure; [Section 10(a)(1)(iii)] and		
d. the consumer has not opted out? [Section 10(a)(1)(iv)] *NOTE: this disclosure limitation applies to consumers as well as to customers [Section 10(b)(1)], and to all nonpublic personal information regardless of whether the information was collected before or after receiving an opt out direction. [Section 10(b)(2)]*		
43. Does the institution provide the consumer with a reasonable opportunity to opt out such as by:		
a. mailing the notices required by Section 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; [Section 10(a)(3)(i)]		
b. where the consumer opens an on-line account with the institution and agrees to receive the notices required by Section 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; [Section 10(a)(3)(ii)] or		
c. for isolated transactions, providing the notices required by Section 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 the completion of the transaction? [Section 10(a)(3)(iii)]		
44. 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? [Section 10(c)] *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 Innformation		
45. If the institution receives information from a nonaffiliated financial institution under an exception in Section 14 or Section 15, does the institution refrain from using or disclosing the information except:		
a. to disclose the information to the affiliates of the financial institution from which it received the information; [Section 11(a)(1)(i)]		
b. to disclose the information to its own affiliates, which are in turn limited by the same disclosure and use restrictions as the recipient institution; [Section 11(a)(1)(ii)] and		
c. to disclose and use the information pursuant to an exception in Section 14 or Section 15 in the ordinary course of business to carry out the activity covered by the exception under which the information was received? [Section 11(a)(1)(iii)] *NOTE: the disclosure or use described in section 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 the phrase "in the ordinary course of business" does not include marketing. [Section 11(a)(2)]*		

Examination Checklist Subpart B	Yes	No
46. If the institution receives information from a nonaffiliated financial institution other than under an exception in Section 14 or Section 15, does the institution refrain from disclosing the information except:		
a. to the affiliates of the financial institution from which it received the information; [Section 11(b)(1)(i)]		
b. to its own affiliates, which are in turn limited by the same disclosure restrictions as the recipient institution; [Section 11(b)(1)(ii)] and		
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? [Section 11(b)(1)(iii)]		
Limits on Sharing Account Number Innformation for Marketing Purposes		
47. 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:		
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; [Section 12(b)(1)] or		
b. to a participant in a private label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program? [Section 12(b)(2)] *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. [Section 12(c)(1)] A transaction account does not include an account to which third parties cannot initiate charges. [Section 12(c)(2)]*		

Examination Checklist Subpart C	Yes	No
Exception to Opt Out Requirements for Providers and Joint Marketing		
48. 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 Section 7 and Section 10, and the revised notice requirements in Section 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 13); [Section 13(a)(1)]		
b. the institution has provided consumers with the initial notice; [Section 13(a)(1)(i)] and		
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 14 or Section 15 in the ordinary course of business to carry out those purposes? [Section 13(a)(1)(ii)]		
Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions		
49. If the institution discloses nonpublic personal information to nonaffiliated third parties, do the requirements for initial notice in Section 4(a)(2), opt out in Sections 7 and 10, revised notice in Section 8, and for service providers and joint marketing in Section 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:		
a. servicing or processing a financial product or service requested or authorized by the consumer; [Section 14(a)(1)]		
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; or [Section 14(a) (2)]		
c. a proposed or actual securitization, secondary market sale (including sale of servicing rights) or other similar transaction related to a transaction of the consumer? [Section 14(a)(3)]		
50. If the institution uses a Section 14 exception as necessary to effect, administer, or enforce a transaction, is the disclosure:		
a. required, or is 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; [Section 14(b)(1)] or		
b. required, or is a usual, appropriate, or acceptable method, to:[Section 14(b)(2)]		
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; [Section 14(b)(2)(i)]		
ii. administer or service benefits or claims; [Section 14(b)(2)(ii)]		
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; [Section 14(b)(2)(iii)]		
iv. accrue or recognize incentives or bonuses; [Section 14(b)(2)(iv)]		
v. underwrite insurance or for reinsurance or for certain other purposes related to a consumer's		

Examination Checklist Subpart C	Yes	No
insurance; [Section 14(b)(2)(v)] or		
vi. in connection with:		
(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; [Section 14(b)(2)(vi)(A)]		
(2) the transfer of receivables, accounts or interests therein; [Section 14(b)(2)(vi)(B)] or		
(3) the audit of debit, credit, or other payment information? [Section 14(b)(2)(vi)(C)]		
Other Exceptions to Notice and Opt Out Requirements		
51. If the institution discloses nonpublic personal information to nonaffiliated third parties, do the requirements for initial notice in Section 4(a)(2), opt out in Sections 7 and 10, revised notice in Section 8, and for service providers and joint marketers in Section 13, not apply because the institution makes the disclosure:		
a. with the consent or at the direction of the consumer; [Section 15(a)(1)]		
b. to protect the confidentiality or security of records, [Section15(a)(2)(i)]; to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability, [Section15(a)(2)(ii)]; for required institutional risk control or for resolving consumer disputes or inquiries, [Section15(a)(2)(iii)]; to persons holding a legal or beneficial interest relating to the consumer, [Section15(a)(2)(iv)]; or to persons acting in a fiduciary or representative capacity on behalf of the consumer; [Section15(a)(2)(v)]		
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; [Section15(a)(3)]		
i. to protect the confidentiality or security of records; [Section 15(a)(2)(i)]		
ii. to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; [Section 15(a)(2)(ii)]		
iii. for required institutional risk control or for resolving consumer disputes or inquiries; [Section 15(a)(2)(iii)]		
iv. to persons holding a legal or beneficial interest relating to the consumer; [Section 15(a)(2)(iv)] or		
v. to persons acting in a fiduciary or representative capacity on behalf of the consumer; [Section 15(a) (2)(v)]		
d. as specifically permitted or required by other provisions of law and in compliance with the Right to Financial Privacy Act, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety; [Section15(a)(4)]		
e. to a consumer reporting agency in accordance with the FCRA or from a consumer report reported by a consumer reporting agency; [Section 15(a)(5)]		
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 solely consumers of such business or unit; [Section 15(a)(6)]		

Examination Checklist Subpart C	Yes	No
g. to comply with Federal, state, or local laws, rules, or legal requirements; [Section 15(a)(7)(i)]		
h. to comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities; [Section 15(a)(7)(ii)] or		
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? [Section 15(a)(7)(iii)] *NOTE: the regulation gives the following as an example of the exception described in section a of this question: "A consumer may specifically consent to [an institution's] 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."*		