RESCINDED

OCC 2001-26

Subject: Privacy of Consumer Financial Information; 12 CFR 40
Date: May 25, 2001

To: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

Description: Examination Procedures

OCC 2001-26 has been replaced by Comptroller's Handbook - Other Consumer Protection Laws and Regulations.

share their nonpublic personal information with third parties (opt-out). The Federal Financial Institutions Examination Council has approved uniform examination procedures to verify compliance with the implementing regulations. A copy of the examination procedures is attached.

OCC examiners will use the procedures during compliance examinations of all national banks, and federal branches and agencies of foreign banks. The examination procedures are risk-based and allow examiners to tailor the examination scope according to the reliability of the bank's compliance management system and the level of risk assumed by the institution. As the initial step, the procedures direct an examiner to gain an understanding of the institution's information-sharing practices and management controls and systems over privacy. Based on that information and using the decision trees provided, the examiner will select the examination modules and applicable procedures that reflect the types of information-sharing practices of the institution. For example, Module 1 is used in institutions with the most complex information-sharing practices, and Module 3 is used in institutions with the least complex information-sharing practices. In addition, examiners will complete modules 1, 5, or 6 depending upon whether the institution receives nonpublic personal information from financial institutions or shares account numbers for marketing purposes.

Notwithstanding the risk-based approach outlined in the procedures, the first compliance examination for each institution conducted after July 1, 2001, will include some transactional testing. At a minimum, during these first privacy examinations, examiners will perform the Initial Procedures and the mandatory procedures listed below from each of the modules applicable to the bank. Examiners will sample transactions to complete the procedures. The amount of sampling will depend upon the reliability of the bank's compliance management system and the level of risk assumed by the institution.

Module	Mandatory	Optional
Module 1	A, B1, C1, C2, C2d	B2, C2a, C2b, Checklist
Module 2	A, B1	B2, Checklist
Module 3	A, B1	B2, Checklist
Module 4	B	A, Checklist
Module 5	B	A, Checklist
Module 6	A, B	C, Checklist

This minimum scope process will be used in the first privacy examination of each institution, including those with reliable and fully implemented privacy programs. In situations where banks have not fully implemented their privacy controls and systems (e.g., completed a privacy audit) or have inadequate systems, examiners should determine, through completion of the Initial Procedures, which optional procedures should be performed in addition to the mandatory procedures.

The OCC plans to incorporate these procedures in an update to the *Comptroller's Handbook* series. Until the revised handbook is issued, examiners will use the attached procedures. Questions about the privacy regulation or these procedures may be directed to your supervisory office or to the Community and Consumer Policy Division at (202) [illegible]428.

Ralph E. Sharpe
Deputy Comptroller
Community and Consumer Policy

Related Links

- Privacy Examination Procedures

Privacy of Consumer Financial Information Table of Contents

Privacy of Consumer Financial Information — Introduction

Background and Overview

On November 12, 1999, President Clinton signed into law the Gramm-Leach-Bliley Act (the Act). Title V, Subtitle A of the Act 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 the institution satisfies various notice and opt-out requirements, and provided that 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.

Accordingly, on June 1, 2000, the four federal bank and thrift regulators[1] published substantively identical regulations implementing provisions of the Act governing the privacy of consumer financial information. The regulations establish rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information, as summarized below (a more complete discussion appears later in this document):

- A financial institution must provide a notice of its privacy policies, 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 regulations.

- Regardless of whether a financial institution shares nonpublic personal information, the institution must provide notices of its privacy policies to its customers.

- A financial institution generally may not disclose customer account numbers to any nonaffiliated third party for marketing purposes.

- A financial institution must follow reuse and redisclosure limitations on any nonpublic personal information it receives from a nonaffiliated financial institution.

The privacy regulations became effective on November 13, 2000. Compliance is required as of July 1, 2001.

Definitions and Key Concepts

In discussing the duties and limitations imposed by the regulations, a number of key concepts are used. These concepts include "financial institution"; "nonpublic personal

[1] These regulators are the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.

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 regulations.

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.[2]

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 made available lawfully to the general public from government records, widely distributed media, or legally required disclosures to the general public. Examples include information in a published telephone book or a publicly recorded document, such as a mortgage or securities filing.

Nonpublic personal information may include individual items of information as well as lists of information. For example, 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).

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

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 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 where the mortgages are recorded in 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 the customers on that list without having to provide notice or opt out (see below for definition).

***Nonaffiliated Third Party*:**

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

***Opt-Out Right and Exceptions*:**

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 regulations 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 allowed 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, again depending on the

circumstances surrounding the consumer's transaction. It is not reasonable to require a consumer to write his or her own letter as the only means to opt out.

The Exceptions

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

- To a nonaffiliated third party to perform services for the financial institution or to function on its behalf, including marketing the institution's own products or services or those offered jointly by the institution and another financial institution. The exception is permitted only if the financial institution provides notice of these arrangements and by contract prohibits the third party from disclosing or using the information for other than the specified purposes. The contract for a joint marketing agreement must provide that the parties to the agreement are jointly offering, sponsoring, or endorsing a financial product or service. However, if the service or function is covered by the exceptions in section 14 or 15 (discussed below), the financial institution need not comply with the additional disclosure and confidentiality requirements of section 13. Disclosure under this exception could include the outsourcing of marketing to an advertising company. (Section 13)

- As necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or under certain other circumstances relating to existing relationships with customers. Disclosures under this exception could be in connection with the audit of credit information, administration of a rewards program, or to provide an account statement. (Section 14)

- For specified other disclosures that a financial institution normally makes, such as to protect against or prevent actual or potential fraud; to the financial institution's attorneys, accountants, and auditors; or to comply with applicable legal requirements, such as the disclosure of information to regulators. (Section 15)

***Consumer* and *Customer*:**

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

A "consumer" is a person, or that person'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.

A consumer who is not a customer is entitled to an initial privacy and opt-out notice only if his or her financial institution wants to share his or her nonpublic personal information with nonaffiliated third parties outside the exceptions.

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 a person purchases a bank check from a financial institution where the person has no account, the person will be a consumer but

not a customer of that institution because he or she has not established a customer relationship. Likewise, if a person uses the automated teller machine (ATM) of a financial institution where that person has no account, even repeatedly, the person will be a consumer, but not a customer of that institution.

Financial Institution Duties

The regulations establish specific duties and limitations for a financial institution based on its activities. Financial institutions that intend to disclose nonpublic personal information outside the exceptions 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 to their customers. 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 regulations.

Notice and Opt-Out Duties to Consumers:

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

- An initial notice of its privacy policies;
- 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.

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. 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.

***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 regulations 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 regulations do not prescribe specific methods for making a notice clear and conspicuous, but do 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 Internet 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 may be able to retain or subsequently access the notice. A written notice satisfies this requirement. For customers who obtain financial products or services electronically and agree to receive their notices on the institution's Web site, the institution may provide the current version of its privacy notice on its Web site.

Notice Content. A privacy notice must contain specific disclosures. However, a financial institution may provide to consumers who are not 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:

- Categories of information collected.
- Categories of information disclosed.
- Categories of affiliates and nonaffiliated third parties to whom the institution may disclose information.
- Policies with respect to the treatment of former customers' information.
- Information disclosed to service providers and joint marketers (Section 13).
- An explanation of the opt-out right and methods for opting out.
- Any opt-out notices the institution must provide under the Fair Credit Reporting Act with respect to affiliate information sharing.
- Policies for protecting the security and confidentiality of information.

- A statement that the institution makes disclosures to other nonaffiliated third parties as permitted by law (Sections 14 and 15).

Limitations on Disclosure of Account Numbers:

A financial institution must not disclose an account number or similar form of access number or access code for a credit card, deposit, 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). Also not barred are disclosures to participants in private-label or affinity card programs, where the participants are identified to the customer when the customer enters the program.

Redisclosure and Reuse Limitations on Nonpublic Personal Information Received:

If a financial institution receives nonpublic personal information from a nonaffiliated financial institution, 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.
  - 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 using it 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;

- Its own affiliates, who may, in turn, disclose the information only to the extent that the financial institution can do so; and

- Any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which it received the information. For example, an institution that received a customer list from another financial institution could disclose the list (1) in accordance with the privacy policy of the financial institution that provided the list, (2) subject to any opt-out election or revocation by the consumers on the list, and (3) in accordance with appropriate exceptions under sections 14 and 15.

Other Matters

Fair Credit Reporting Act

The regulations do not modify, limit, or supersede the operation of the Fair Credit Reporting Act.

State Law

The regulations do not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that it is inconsistent with the regulations. A state statute, regulation, order, or interpretation is consistent with the regulations if the protection it affords any consumer is greater than the protection provided under the regulations, as determined by the FTC.

Grandfathered Service Contracts

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

Guidelines Regarding Protecting Customer Information

The regulations require 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 bank and thrift regulators have published guidelines, pursuant to section 501(b) of the Gramm-Leach-Bliley Act, that address steps that a financial institution should take in order to protect customer information. The guidelines relate only to information about customers, rather than all consumers. Compliance examiners should consider the findings of a 501(b) inspection during the compliance examination of a financial institution for purposes of evaluating the accuracy of the institution's disclosure regarding data security.

Privacy of Consumer Financial Information — Examination Objectives

1. Assess the quality of a financial institution's compliance management policies and procedures for implementing the privacy 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. Determine the reliance that can be placed on a financial institution's internal controls and procedures for monitoring the institution's compliance with the privacy regulation.

3. Determine a financial institution's compliance with the privacy 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 that are 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 regulations.

4. Initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

Privacy of Consumer Financial Information — Initial Procedures

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; its treatment of nonpublic personal information; and its administration of opt-outs. Consider the following as appropriate:

1. Notices (initial, annual, revised, opt-out, short-form, and simplified).

2. Institutional privacy policies and procedures, including those to:

   - Process requests for nonpublic personal information, including requests for aggregated data.
   - Deliver notices to consumers.
   - Manage consumer opt-out directions (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.
   - 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 the data collected electronically through Internet cookies; or through ATM transactions).

6. Categories of nonpublic personal information shared with, or received from, each nonaffiliated third party.

7. Consumer complaints regarding the treatment of nonpublic personal information, including 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. Results of a 501(b) inspection (used to determine the accuracy of the institution's privacy disclosures regarding data security).

B. Use the information gathered 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 Reuse and Redisclosure and Account Number Sharing Decision Trees, as necessary (Attachments B & C). Identify which module is applicable.

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

1. Sufficiency of internal policies and procedures and 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.

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 instruction 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.

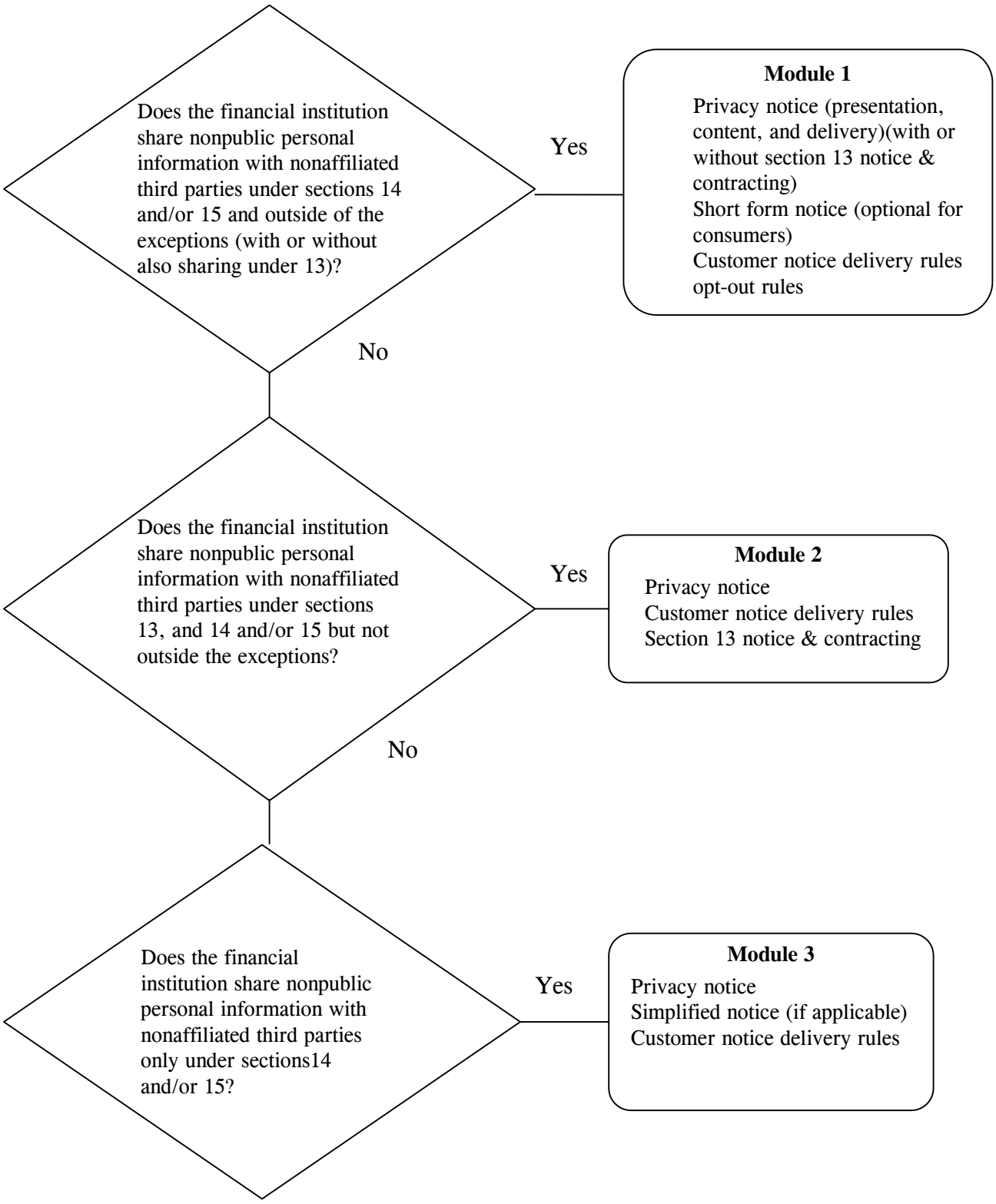
1. Summarize all findings.

2. For violation(s) noted, determine the cause by identifying weaknesses in internal controls, compliance review, training, management oversight, or other areas.

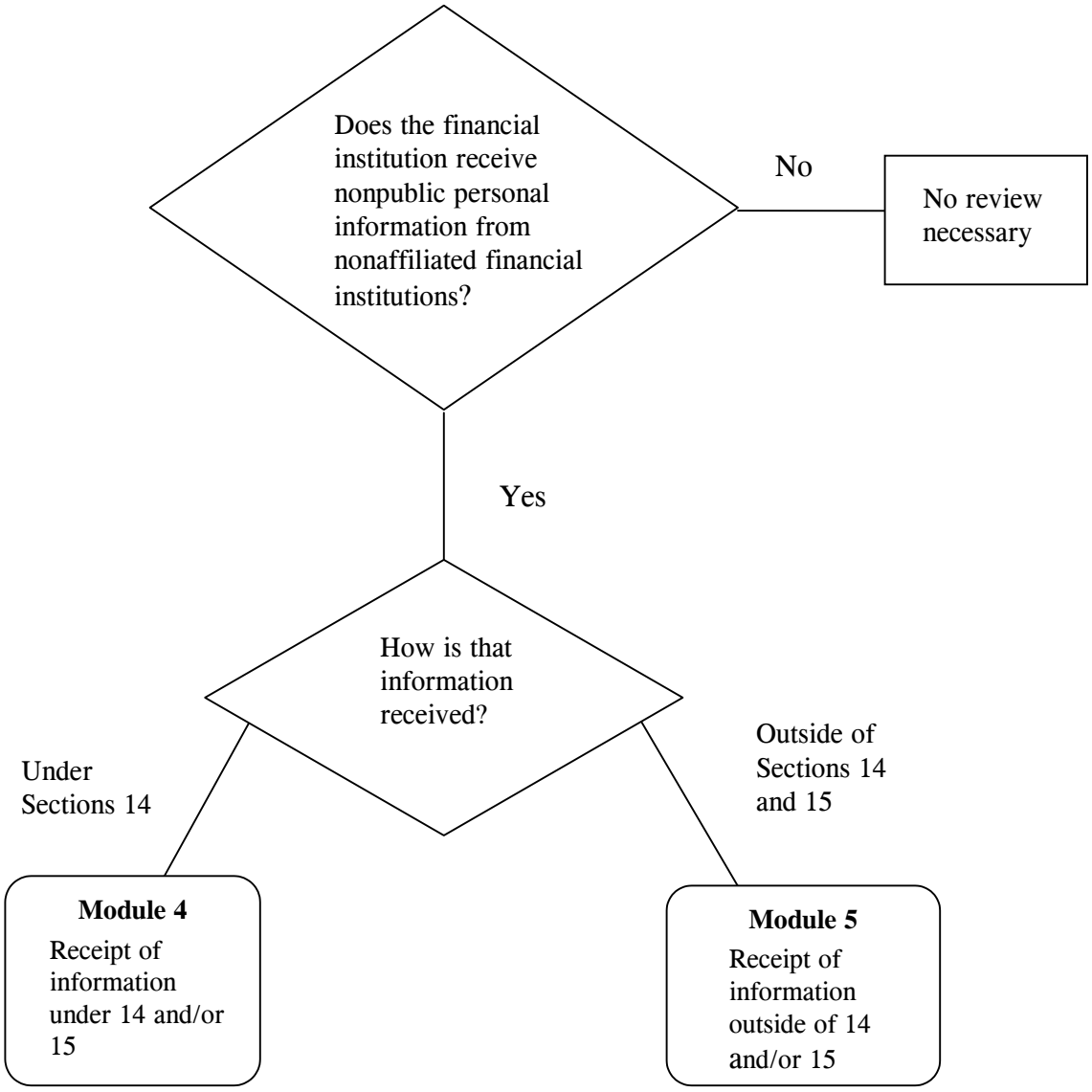
3. Identify action needed to correct violations and weaknesses in the institution's compliance system, as appropriate.

4. Discuss findings with management and obtain a commitment for corrective action.

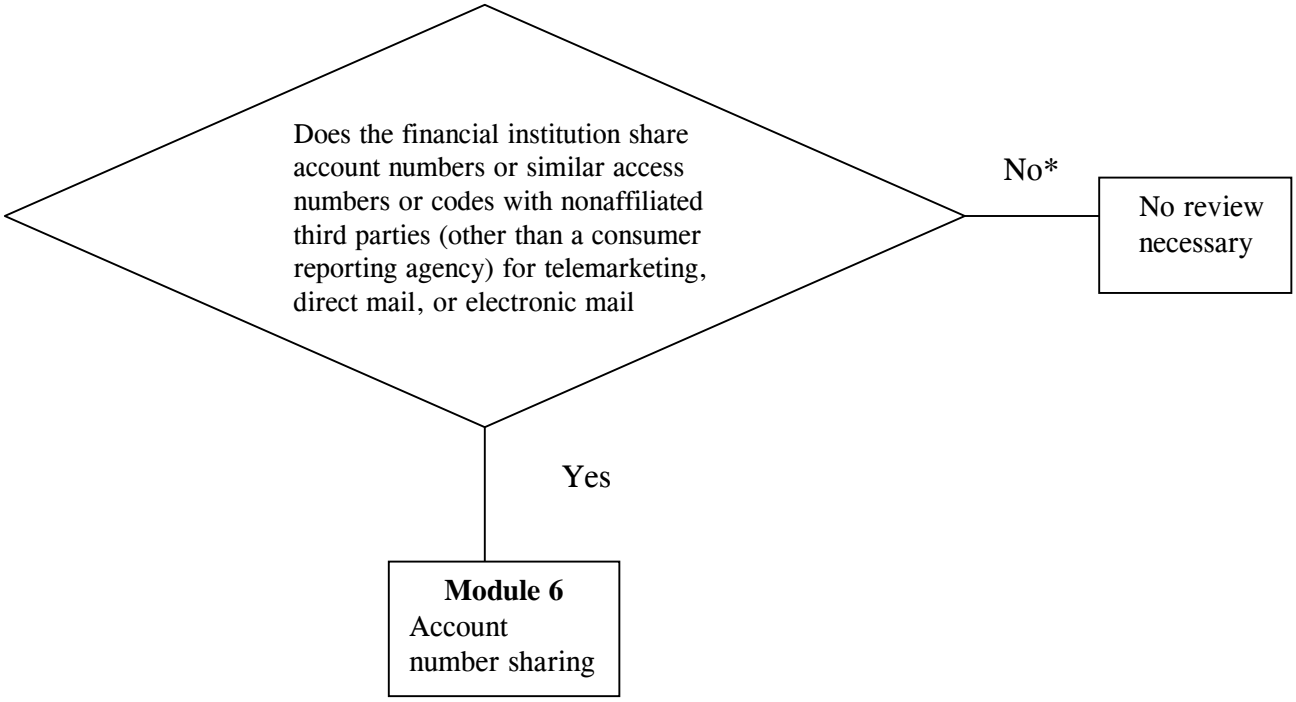
PRIVACY NOTICE AND OPT-OUT DECISION TREE



REUSE & REDISCLOSURE 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.

Sharing nonpublic personal information with nonaffiliated third parties under Sections 14 and/or 15 and outside the exceptions (with or without also sharing under Section 13).

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

A. Disclosure of Nonpublic Personal Information

1. Select a sample of third-party relationships with nonaffiliated third parties and obtain a sample of data shared between the institution and the third party both inside and outside of the exceptions. The sample should include a cross-section of relationships, emphasizing 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 data shared and with whom the data were shared to those stated in the privacy notice and verify that what the institution tells consumers (customers and those who are not customers) in its notices about its policies and practices in this regard and what the institution actually does are consistent (12 CFR 40.10, 40.6).

    b. Compare the data 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 (12 CFR 40.10).

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. Note that the "grandfather" provisions of Section 18 apply to certain of these contracts (12 CFR 40.13(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 (12 CFR 40.3(b), 40.4(a), 40.5(a)(1), 40.8(a)(1));

b. Accurately reflect the policies and practices used by the institution (12 CFR 40.4(a), 40.5(a)(1), 40.8(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 and contain examples as applicable (12 CFR 40.6). Note that if the institution shares under Section 13, the notice provisions for that section shall also apply.

2. Through discussions with management, review of the institution's policies and procedures, and a sample of electronic or written consumer records where available, determine whether the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:

a. Timeliness of delivery (12 CFR 40.4(a), 40.7(c), 40.8(a)); and

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) (12 CFR 40.9).

c. For customers only, review the timeliness of delivery (12 CFR 40.4(d), 40.4(e), 40.5(a)), means of delivery of annual notice (12 CFR 40.9(c)), and accessibility of or ability to retain the notice (12 CFR 40.9(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 (12 CFR 40.3(b) and 40.7(a)(1)).

b. Accurately explain the right to opt out (12 CFR 40.7(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) (12 CFR 40.7(a)(1)).

d. Describe how the institution treats joint consumers (customers and those who are not customers), as applicable (12 CFR 40.7(d)).

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

   a. Timeliness of delivery (12 CFR 40.10(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) (12 CFR 40.9).

   c. Reasonableness of the opportunity to opt out (the time allowed to and the means by which the consumer may opt out) (12 CFR 40.10(a)(1)(iii), 40.10(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 (12 CFR 40.7(e), 40.7 (f), 40.7 (g)).

D. Checklist Cross-references

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, 40
4(a, c, d, e); 5; and 9(c, e)	Customer notice delivery rules	1, 3-7, 37, 38
13	Section 13 notice and contracting rules (as applicable)	12, 47
6(d)	Short-form notice rules (optional for consumers only)	15-17
7; 8; and 10	Opt-out rules	19-34, 41-43
14; 15	Exceptions	48, 49, 50

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 data shared between the institution and the third party. The sample should include a cross-section of relationships emphasizing 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 data shared and with whom the data were shared to ensure that the institution accurately categorized its information-sharing practices and is not sharing nonpublic personal information outside the exceptions (12 CFR 40.13, 40.14, 40.15).

    b. Compare the categories of data shared and with whom the data were 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 (12 CFR 40.10, 40.6).

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. Note that the "grandfather" provisions of Section 18 apply to certain of these contracts. (12 CFR 40.13(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 (12 CFR 40.3(b), 40.4(a), 40.5(a)(1));

    b. Accurately reflect the policies and practices used by the institution (12 CFR 40.4(a), 40.5(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 and contain examples as applicable (12 CFR 40.6, 40.13).

2. Through discussions with management, review of the institution's policies and procedures, and a sample of electronic or written consumer records where available, determine whether the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:

   a. Timeliness of delivery (12 CFR 40.4(a)); and

   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) (12 CFR 40.9).

   c. For customers only, review the timeliness of delivery (12 CFR 40.4(d), 40.4(e), and 40.5(a)), means of delivery of annual notice 12 CFR 40.9(c)), and accessibility of or ability to retain the notice (12 CFR 40.9(e)).

C. Checklist Cross-references

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, 40
13	Section 13 notice and contracting rules	12, 47
4(a, c, d, e); 5; and 9(c, e)	Customer notice delivery rules	1, 3-7, 37, 38
14; 15	Exceptions	48, 49, 50

Privacy of Consumer Financial Information — 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 data shared between the institution and the third party.

    a. Compare the data shared and with whom the data were shared to ensure that the institution accurately states its information-sharing practices and that it 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 (12 CFR 40.3(b), 40.4(a), 40.5(a)(1)).

    b. Accurately reflect the policies and practices used by the institution (12 CFR 40.4(a), 40.5(a)(1)). Note, this includes practices disclosed in the notices that exceed regulatory requirements.

    c. Include, and adequately describe, all required items of information (12 CFR 40.6).

2. Through discussions with management, review of the institution's policies and procedures, and a sample of electronic or written customer records where available, determine if the institution has adequate procedures in place to provide notices to customers, as appropriate. Assess the following:

    a. Timeliness of delivery (12 CFR 40.4(a), 40.4(d), 40.4(e), 40.5(a)).

    b. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the customer agrees; or as a necessary step of a transaction) (12 CFR 40.9) and accessibility of or ability to retain the notice (12 CFR 40.9(e)).

C. Checklist Cross-references

Regulation Section	Subject	Checklist Questions
6	Customer notice content and presentation	8-11, 14, 18
6 (c)(5)	Simplified notice content (optional)	13
4 (a, d, e); 5; and 9	Customer notice delivery process	1, 3-7, 35-40
14; 15	Exceptions	48, 49, 50

Reuse and redisclosure of 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 procedures, determine whether the institution has adequate practices to prevent the unlawful redisclosure and reuse of the information where the institution is the recipient of nonpublic personal information (12 CFR 40.11(a)).

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

1. Verify that the institution'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 (12 CRF 40.11(a)(1)(i) and (ii)).

2. Verify that the institution only uses and shares the data pursuant to an exception in sections 14 and 15 (12 CRF 40.11(a)(1)(iii)).

C. Checklist Cross-references

Regulation Section	Subject	Checklist Question
11(a)	Reuse and redisclosure	44

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 procedures, determine whether the institution has adequate practices to prevent the unlawful redisclosure of the information where the institution is the recipient of nonpublic personal information (12 CFR 40.11(b)).

B. Select a sample of data received from nonaffiliated financial institutions and shared with others to evaluate the financial institution's compliance with 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 b below (§11(b)(1)(i) and (ii)).

2. If the institution shares information with entities other than those under step a above, verify that the institution's information-sharing practices conform to those in the nonaffiliated financial institution's privacy notice (§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 (12 CFR 40.10, 40.11(b)(1)(iii)).

C. Checklist Cross-references

Regulation Section	Subject	Checklist Question
11(b)	Reuse and redisclosure	45

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 (12 CFR 40.12).

B. Obtain and review a sample of contracts with agents or service providers to whom the financial institution discloses account numbers for use in connection with marketing the institution's own products or services. Determine whether the institution shares account numbers with nonaffiliated third parties only to perform marketing for the institution's own products and services. Ensure that the contracts do not authorize these nonaffiliated third parties to initiate charges directly to customer's accounts (12 CFR 40.12(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 whether the participants in each program are identified to the customer when the customer enters into the program (12 CFR 40.12(b)(2)).

D. Checklist Cross-references

Regulation Section	Subject	Checklist Question
12	Account number sharing	46

Privacy of Consumer Financial Information Examination Checklist

Yes	No	

SUBPART A
Initial Privacy Notice

1. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to *all customers* not later than when the customer relationship is established, other than as allowed in 12 CFR 40.(4)(e)? [12 CFR 40.4(a)(1))]

(*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. [12 CFR 40.4(b)] With respect to credit relationships, an institution establishes a customer relationship when it originates a consumer loan. If the institution subsequently sells the servicing rights to the loan to another financial institution, the customer relationship transfers with the servicing rights. [12 CFR 40.4(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 12 CFR 40.14 or 15? [12 CFR 40.4(a)(2)]

3. Does the institution provide to *existing customers* who obtain a new financial product or service an initial privacy notice that covers the customer's new financial product or service, if the most recent notice provided to the customer was not accurate with respect to the new financial product or service? [12 CFR 40.4(d)(1)]

4. Does the institution provide initial notice *after establishing a customer relationship* only:
   a) If the customer relationship is not established at the customer's election? [12 CFR 40.4(e)(1)(i)]

   -or-

   b) If to 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? [12 CFR 40.4 (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? [12 CFR 40.4(e)]

Privacy of Consumer Financial Information Examination Checklist

Yes	No	
		Annual Privacy Notice 6. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices at least annually (that is, at least once in any period of 12 consecutive months) to all customers, throughout the customer relationship? [12 CFR 40.5(a)(1)and 40.(2)] (*Note:* annual notices are not required for former customers. [12 CFR 40.5(b)(1)and (2)])

Yes	No	
		7. Does the institution provide an annual privacy notice to each customer whose loan the institution owns the right to service? [12 CFR 40.5(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; [12 CFR 40.6(a)(1)] b. The categories of nonpublic personal information that the institution discloses; [12 CFR 40.6(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 12 CFR 40.14 or 40.15; [12 CFR 40.6(a)(3)] 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 12 CFR 40.14 or 40.15; [12 CFR 40.6(a)(4)] e. If the institution discloses nonpublic personal information to a nonaffiliated third party under 12 CFR 40.13, and no exception under 12 CFR 40.14 or 40.15 applies, a separate statement of the categories of information the institution discloses and the categories of third parties with whom the institution has contracted; [12 CFR 40.6(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; [12 CFR 40.6(a)(6)]

		g. Any disclosures that the institution makes under 12 CFR 40.603(d)(2)(A)(iii) of the Fair Credit Reporting Act (FCRA); [12 CFR 40.6(a)(7)] h. The institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; [12 CFR 40.6(a)(8)] and i. A general statement–with no specific reference to the exceptions or to the third parties–that the institution makes disclosures to other nonaffiliated third parties as permitted by law*?* [12 CFR 40.6(a)(9), (b)] (*Note:* sample clauses for these items appear in Appendix A of the Regulation.) 9. If an institution collects nonpublic personal information in any of the following categories, does it list that category of information? a. From the consumer?[12 CFR 40.6(c)(1)(i)] b. About the consumer's transactions with the institution or its affiliates? [12 CFR 40.6(c)(1)(ii)] c. About the consumer's transactions with nonaffiliated third parties? [12 CFR 40.6(c)(1)(iii)] d. From a consumer reporting agency? [12 CFR 40.6(c)(1)(iv)]
Yes	**No**	10. If an institution collects nonpublic personal information in any of the following categories, does it list that category of information and give a few examples from each category (or if it does not list the categories it collects and give examples, does it state that it reserves the right to disclose all the nonpublic personal information that it collects)? a. From the consumer? b. About the consumer's transactions with the institution or its affiliates? c. About the consumer's transactions with nonaffiliated third parties? d. From a consumer reporting agency? [12 CFR 40.6(c)(2)] (*Note*: examples are recommended under 12 CFR 40.6(c)(2) although not under 12 CFR 40.6(c)(1).) 11. Does the institution list the following categories of affiliates and nonaffiliated third parties to whom it discloses information, as applicable, while providing a few specific examples of the third parties in each category: a. Financial service providers? [12 CFR 40.6(c)(3)(i)] b. Non-financial companies? [12 CFR 40.6(c)(3)(ii)] c. Others? [12 CFR 40.6(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 12 CFR 40.13: a. As applicable, the same categories and examples of nonpublic personal information disclosed as described in paragraphs 12 CFR 40.6 (a)(2) and 40.(c)(2)(see questions 8b and 10) and [12 CFR 40.6(c)(4)(i)]? 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? [12 CFR 40.6(c)(4)(ii)(A)] c. That the third party is a financial institution with which the institution has a joint marketing agreement? [12 CFR 40.6(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 12 CFR 40.14 and 40.15, 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? c. The policies and practices the institution uses to protect the confidentiality and security of nonpublic personal information? d. A general statement that the institution makes disclosures to other nonaffiliated third parties as permitted by law? [12 CFR 40.6(c)(5)] (*Note:* use of this type of simplified notice is optional; an institution may always use a full notice.)
Yes	**No**	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; and [12 CFR 40.6(c)(6)(i)]? b. Whether security practices and policies are in place to ensure the confidentiality of the information in accordance with the institution's policy? [12 CFR 40.6(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? [12 CFR 40.6(d)(1)]

16. If the institution provides a short-form initial privacy notice according to 12 CFR 40.6(d)(1), does the short-form initial notice:
    a. Conform to the definition of "clear and conspicuous?" [12 CFR 40.6(d)(2)(i)]
    b. State that the institution's full privacy notice is available upon request? [12 CFR 40.6(d)(2)(ii)]
    c. Explain a reasonable means by which the consumer may obtain the notice? [12 CFR 40.6(d)(2)(iii)]

(*Note:* The institution is not required to deliver the full privacy notice with the short-form initial notice. [12 CFR 40.6(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? [12 CFR 40.6(d)(4)(i)]
    b. For the consumer who conducts business in person at the institution's office, having copies on hand and available immediately by hand-delivery? [12 CFR 40.6(d)(4)(ii)]

18. If the institution, in its privacy policies, reserves the right to disclose nonpublic personal information to nonaffiliated third parties in the future, does the privacy notice include, as applicable:
    a. Categories of nonpublic personal information that the financial institution reserves the right to disclose in the future, but does not currently disclose? [12 CFR 40.6(e)(1)]
    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? [12 CFR 40.6(e)(2)]

Privacy of Consumer Financial Information Examination Checklist

Yes	No	
		Opt-Out Notice 19. If the institution discloses nonpublic personal information about a consumer to a nonaffiliated third party, and the exceptions under 12 CFR 40.13-40.15 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? [12 CFR 40.7(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? [12 CFR 40.7(a)(1)(i)] b. That the consumer has the right to opt out of that disclosure; [12 CFR 40.7(a)(1)(ii)] and c. A reasonable means by which the consumer may opt out? [12 CFR 40.7(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? [12 CFR 40.7(a)(2)(i)(A)] b. All the categories of nonaffiliated third parties to whom the information is disclosed? [12 CFR 40.7(a)(2)(i)(A)] c. That the consumer has the right to opt out of the disclosure of that information? [12 CFR 40.7(a)(2)(i)(A)] d. The financial products or services that the consumer obtains to which the opt-out direction would apply? [12 CFR 40.7(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? [12 CFR 40.7(a)(2)(ii)(A)] b. A reply form included with the opt-out notice? [12 CFR 40.7(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? [12 CFR 40.7(a)(2)(ii)(C)] or d. A toll-free telephone number? [12 CFR 40.7(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. [12 CFR 40.7(a)(iv)])

		23. If the institution delivers the opt-out notice after the initial notice, does the institution provide the initial notice once again with the opt-out notice? [12 CFR 40.7(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? [12 CFR 40.7(d)(1)]

Yes	**No**	
		25. Does the institution permit each of the joint consumers in a joint relationship to opt out? [12 CFR 40.7(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; [12 CFR 40.7(d)(2)(i)] or b. Each joint consumer is permitted to opt out separately? [12 CFR 40.7(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? [12 CFR 40.7(d)(3)] b. The joint consumers to notify the institution in a single response? [12 CFR 40.7(d)(5)] c. Each joint consumer to opt out either for himself or herself, and/or for another joint consumer? [12 CFR 40.7(d)(5)] 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? [12 CFR 40.7(d)(4)] 29. Does the institution comply with a consumer's direction to opt out as soon as is reasonably practicable after receiving it? [12 CFR 40.7(e)] 30. Does the institution allow the consumer to opt out at any time? [12 CFR 40.7(f)] 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? [12 CFR 40.7(g)(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)? [12 CFR 40.7(g)(2)]

Revised Notices

33. Except as permitted by 12 CFR 40.13-40.15, does the institution refrain from disclosing any nonpublic personal information about a consumer to a nonaffiliated third party, other than as described in the initial privacy notice provided to the consumer, unless:
    a. The institution has provided the consumer with a clear and conspicuous revised notice that accurately describes the institution's privacy policies and practices? [12 CFR 40.8(a)(1)]
    b. The institution has provided the consumer with a new opt-out notice? [12 CFR 40.8(a)(2)]
    c. The institution has given the consumer a reasonable opportunity to opt out of the disclosure, before disclosing any information? [12 CFR 40.8(a)(3)]
    d. The consumer has not opted out? [12 CFR 40.8(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? [12 CFR 40.8(b)(1)(i)]
    b. Discloses nonpublic personal information to a new category of nonaffiliated third party? [12 CFR 40.8(b)(1)(ii)]
    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? [12 CFR 40.8(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. [12 CFR 40.8(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? [12 CFR 40.9(a)]

36. Does the institution use a reasonable means for delivering the notices, such as:
    a. Hand-delivery of a printed copy? [12 CFR 40.9(b)(1)(i)]
    b. Mailing a printed copy to the last known address of the consumer? [12 CFR 40.9(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? [12 CFR 40.9(b)(1)(iii)]
    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? [12 CFR 40.9(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. [12 CFR 40.9 (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? [12 CFR 40.9(c)(1)]
    b. For the customer who has requested the institution refrain from sending any information about the customer relationship, making copies of the current privacy notice available upon customer request? [12 CFR 40.9(c)(2)]

38. 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? [12 CFR 40.9(e)(1)]

39. 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? [12 CFR 40.9(e)(2)(i)]
    b. Mailing a printed copy to the last known address of the customer? [12 CFR 40.9(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? [12 CFR 40.9(e)(2)(iii)]

40. Does the institution provide at least one initial, annual, and revised notice, as applicable, to joint consumers? [12 CFR 40.9(g)]

SUBPART B
Limits on Disclosure to Nonaffiliated Third Parties

41. Does the institution refrain from disclosing any nonpublic personal information about a consumer to a nonaffiliated third party, other than as permitted under 12 CFR 40.13-40.15, unless:
    a. It has provided the consumer with an initial notice? [12 CFR 40.10(a)(1)(i)]
    b. It has provided the consumer with an opt-out notice? [12 CFR 40.10(a)(1)(ii)]
    c. It has given the consumer a reasonable opportunity to opt out before the disclosure? [12 CFR 40.10(a)(1)(iii)]
    d. The consumer has not opted out? [12 CFR 40.10(a)(1)(iv)]

(*Note:* This disclosure limitation applies to consumers as well as to customers [12 CFR 40.10(b)(1)], and to all nonpublic personal information regardless of whether collected before or after receiving an opt-out direction. [12 CFR 40.10(b)(2)])

42. Does the institution provide the consumer with a reasonable opportunity to opt out such as by:
    a. Mailing the notices required by 12 CFR 40.10 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? [12 CFR 40.10(a)(3)(i)]
    b. Where the consumer opens an on-line account with the institution and agrees to receive the notices required by 12 CFR 40.10 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? [12 CFR 40.10(a)(3)(ii)]
    c. For isolated transactions, providing the notices required by 12 CFR 40.10 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? [12 CFR 40.10(a)(3)(iii)]

43. Does the institution allow the consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out? [12 CFR 40.10(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 Information

44. If the institution receives information from a nonaffiliated financial institution under an exception in 12 CFR 40.14 or 40.15, 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? [12 CFR 40.11(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? [12 CFR 40.11(a)(1)(ii)]
    c. To disclose and use the information pursuant to an exception in 12 CFR 40.14 or 40.15 in the ordinary course of business to carry out the activity covered by the exception under which the information was received? [12 CFR 40.11(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 "in the ordinary course of business" does not include marketing. [12 CFR 40.11(a)(2)])

45. If the institution receives information from a nonaffiliated financial institution other than under an exception in 12 CFR 40.14 or 40.15, does the institution refrain from disclosing the information except:
    a. To the affiliates of the financial institution from which it received the information? [12 CFR 40.11(b)(1)(i)]
    b. To its own affiliates, which are in turn limited by the same disclosure restrictions as the recipient institution? [12 CFR 40.11(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? [12 CFR 40.11(b)(1)(iii)]

Yes	No	
		Limits on Sharing Account Number Information for Marketing Purposes 46. Does the institution refrain from disclosing, directly or through affiliates, account numbers or similar forms of access numbers or access codes for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party (other than 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? [12 CFR 40.12(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? [12 CFR 40.12(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. [12 CFR 40.12(c)(1)] A transaction account does not include an account to which third parties cannot initiate charges. [12 CFR 40.12(c)(2)]) **SUBPART C** **Exception to Opt-Out Requirements for Service Providers and Joint Marketing** 47. If the institution discloses nonpublic personal information to a nonaffiliated third party without permitting the consumer to opt out, do the opt-out requirements of 12 CFR 40.7 and 40.10, and the revised notice requirements in 40.8, 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 12 CFR 40.13 (b))? [12 CFR 40.13(a)(1)]

		b The institution has provided consumers with the initial notice? [12 CFR 40.13(a)(1)(i)] 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 12 CFR 40.14 or 40.15 in the ordinary course of business to carry out those purposes? [12 CFR 40.13(a)(1)(ii)]

Privacy of Consumer Financial Information Examination Checklist

Yes	No	
		Exceptions to Notice and Opt-Out Requirements for Processing and Servicing Transactions 48. If the institution discloses nonpublic personal information to nonaffiliated third parties, do the requirements for initial notice in 12 CFR 40.4(a)(2), opt-out in 12 CFR 40.7 and 40.10, revised notice in 40.8, and for service providers and joint marketing in 40.13, 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? [12 CFR 40.14(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? [12 CFR 40.14(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? [12 CFR 40.14(a)(3)] 49. If the institution uses a Section 14 exception as necessary to effect, administer, or enforce a transaction, is it : 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? [12 CFR 40.14(b)(1)] b. Required, or is a usual, appropriate, or acceptable method to:[12 CFR 40.14(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? [12 CFR 40.14(b)(2)(i)] ii. Administer or service benefits or claims? [12 CFR 40.14(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? [12 CFR 40.14(b)(2)(iii)] iv. Accrue or recognize incentives or bonuses? [12 CFR 40.14(b)(2)(iv)] v. Underwrite insurance or for reinsurance or for certain other purposes related to a consumer's insurance? [12 CFR 40.14(b)(2)(v)] or

vi. in connection with:
(1) the authorizing, settling, billing, processing, clearing, transferring, reconciling, or collecting 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? [12 CFR 40.14(b)(2)(vi)(A)]
(2) The transfer of receivables, accounts or interests therein? [12 CFR 40.14(b)(2)(vi)(B)] or
(3) The audit of debit, credit, or other payment information? [12 CFR 40.14(b)(2)(vi)(C)]

Other Exceptions to Notice and Opt-Out Requirements

50. If the institution discloses nonpublic personal information to nonaffiliated third parties, do the requirements for initial notice in 12 CFR 40.4(a)(2), opt out in 40.7 and 40.10, revised notice in 40.8, and for service providers and joint marketers in 40.13, not apply because the institution makes the disclosure:
a. With the consent or at the direction of the consumer? [12 CFR 40.15(a)(1)]
b.
i. To protect the confidentiality or security of records? [12 CFR 40.15(a)(2)(i)]
ii. To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability? [12 CFR 40.15(a)(2)(ii)]
iii. For required institutional risk control or for resolving consumer disputes or inquiries? [12 CFR 40.15(a)(2)(iii)]
iv. To persons holding a legal or beneficial interest relating to the consumer? [12 CFR 40.15(a)(2)(iv)] **- or -**
v. To persons acting in a fiduciary or representative capacity on behalf of the consumer? [12 CFR 40.15(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? [12 CFR 40.15(a)(3)]
d. In compliance with the Right to Financial Privacy Act, or to law enforcement agencies? [12 CFR 40.15(a)(4)]
e. To a consumer reporting agency in accordance with the FCRA or from a consumer report reported by a consumer reporting agency? [12 CFR 40.15(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? [12 CFR 40.15(a)(6)]
g. To comply with federal, state, or local laws, rules, or legal requirements? [12 CFR 40.15(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? [12 CFR 40.15(a)(7)(ii)] 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? [12 CFR 40.15(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.")

Privacy of Consumer Financial Information Request Letter Enclosure

The information should be as of *(examination as-of date)*, unless otherwise indicated.

By (insert a date approximately two weeks before the examination starts), please forward to (insert examiner name and address) the following information:

1. Copies of privacy and information security policies and procedures.

2. Describe key internal controls in place to ensure compliance.

3. Copies of any compliance reports, audit reports, audit procedures and board/management responses.

4. Copies of privacy notices (initial, annual, revised, opt-out, short-form, and simplified).

5. List affiliates and nonaffiliated third parties to whom the bank discloses nonpublic personal information about consumers, customers, and former customers:

   - Outside the regulatory exceptions (12 CFR 40.13, 40.14, and 40.15).
   - Under 12 CFR 40.13, including joint marketing agreements.

6. Describe how the bank ensures that nonpublic personal information received from nonaffiliated financial institutions is reused and redisclosed according to regulatory requirements, and describe such sharing activities.

Please provide copies, or have available, on the first day of the exam (insert date):

7. Any records supporting the bank's categorization of its information-sharing practices under 12 CFR 40.13, 40.14, and 40.15, and outside the regulatory exceptions, if available.

8. Information-sharing agreements and contracts between the bank and its affiliates and between the bank and non-affiliated third parties.

9. A listing of consumers and customers who have opted out of disclosure of nonpublic personal information to nonaffiliated third parties.

10. Consumer and customer complaints regarding the treatment of nonpublic personal information.

11. Nonaffiliated third-party complaint logs, telemarketing scripts, and any other information obtained from nonaffiliated third parties, if available.

12. Compliance and audit work papers related to privacy.

13. Training-program information and materials.