

- 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 (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, etc. 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 functions 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.³

³ 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.

The four federal bank and thrift regulators have published guidelines, pursuant to section 501(b) of the Gramm-Leach-Bliley Act, 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 data security.

Examination Objectives

1. To 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. To 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. To 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 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. To initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

Examination 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; how it treats nonpublic personal information; and how it administers opt-outs. Consider the following as appropriate:

VIII. Privacy – GLBA

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; 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 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; and
 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" (page VIII-1.7). Identify which module(s) (beginning on page VIII-1.9) of procedures is (are) applicable.
 - C. Use the information gathered from step A to work through the Reuse and Rediscovery and Account Number Sharing Decision Trees, as necessary (page VIII-1.8). Identify which module (beginning on page VIII-1.13) 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; 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

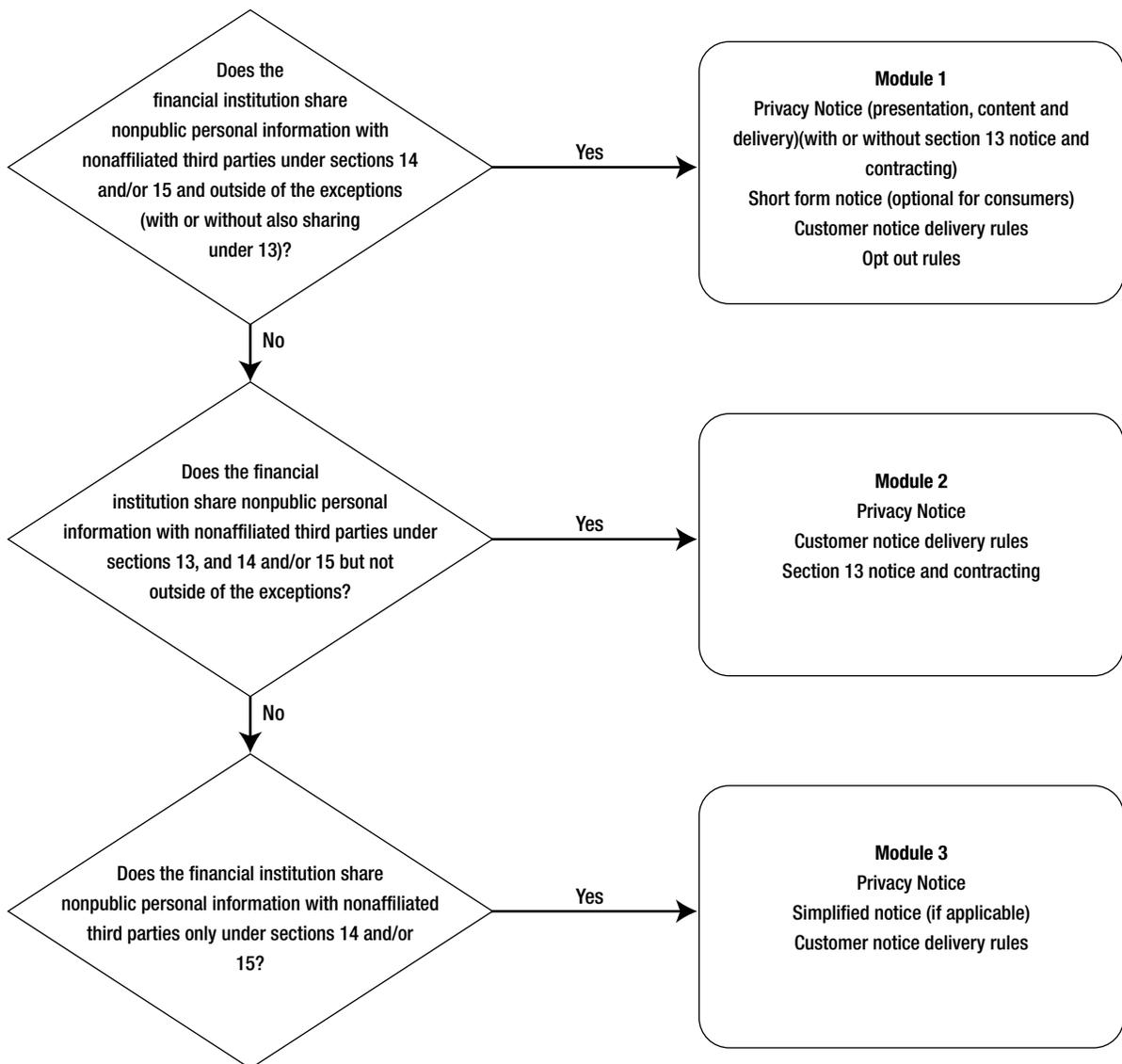
general instruction to verify compliance, cross-referenced to cites within the regulation. Additionally, there are cross-references to a more comprehensive checklist, which the examiner may use if needed to evaluate compliance in more detail.

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.

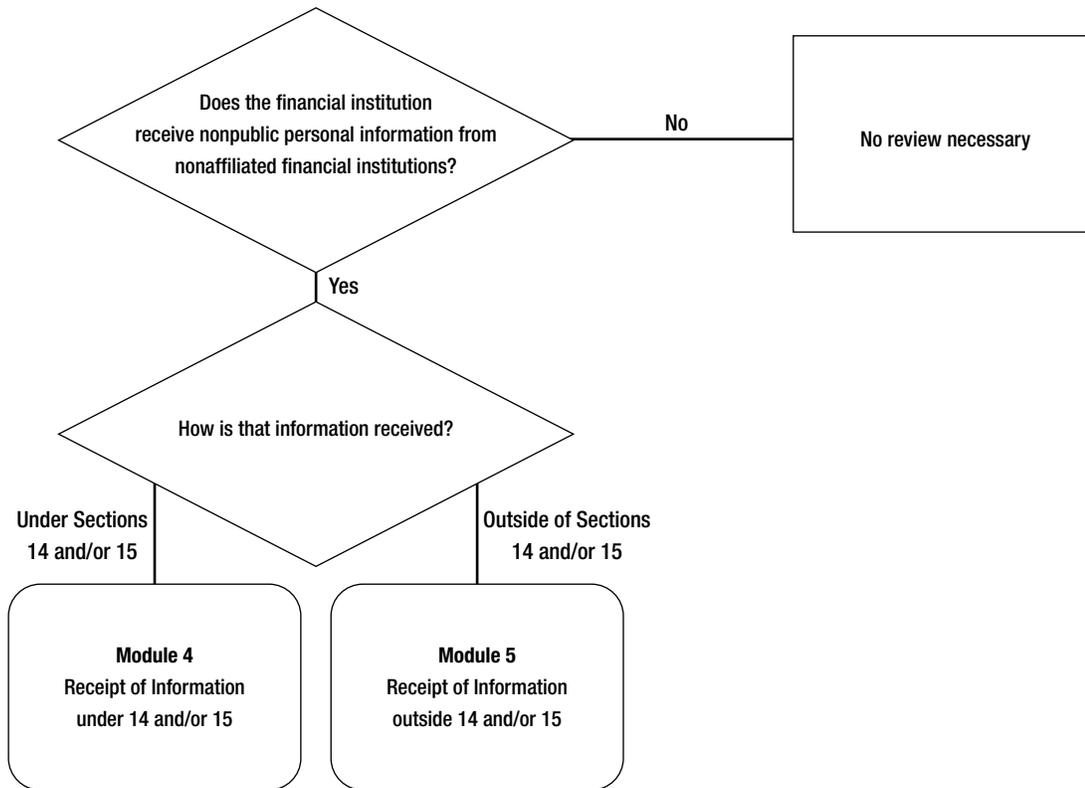
H. Formulate conclusions.

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.

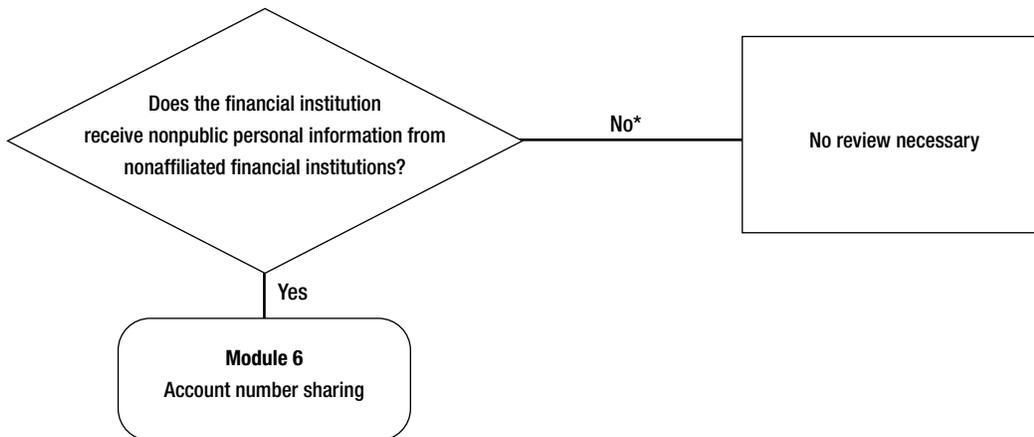
Privacy Notice and Opt Out Decision Tree



Reuse and 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.