

**Module 1**

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

*NOTE: Financial institutions whose practices fall within this category engage in the most expansive degree of information sharing permissible. Consequently, these institutions are held to the most comprehensive compliance standards imposed by the 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 but should emphasize those that are higher risk in nature as determined by the initial procedures. Perform the following comparisons to evaluate the financial institution's compliance with disclosure limitations.
  - a. Compare the categories of 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 (§§10, 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 (§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 (§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 (§§3(b), 4(a), 5(a)(1), 8(a)(1));

- b. Accurately reflect the policies and practices used by the institution (§§4(a), 5(a)(1), 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 (§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 if the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
    - a. Timeliness of delivery (§§4(a), 7(c), 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) (§9).
    - c. For customers only, review the timeliness of delivery (§§4(d), 4(e), 5(a)), means of delivery of annual notice (§9(c)), and accessibility of or ability to retain the notice (§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 (§§3(b) and 7(a)(1));
  - b. Accurately explain the right to opt out (§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) (§7(a)(1)); and
  - d. Describe how the institution treats joint consumers (customers and those who are not customers), as applicable (§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 if the institution has adequate procedures in place to provide the opt out notice and comply with opt out directions of consumers (customers and those who are not customers), as appropriate. Assess the following:
  - a. Timeliness of delivery (§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) (§9); and

## VIII. Privacy – GLBA

---

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

3. 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 (§7(e), (f), (g)).

### D. Checklist Cross References—Module 1

<b>Regulation Section</b>	<b>Subject</b>	<b>Checklist Questions</b>
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