

**Module 2**

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

**A. Disclosure of Nonpublic Personal Information**

1. Select a sample of third party relationships with nonaffiliated third parties and obtain a sample of data shared between the institution and the third party. The sample should include a cross-section of relationships but should emphasize those that are higher risk in nature as determined by the initial procedures. 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 (§§13, 14, 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 (§§10, 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. (§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 (§§3(b), 4(a), 5(a)(1));
  - b. Accurately reflect the policies and practices used by the institution (§§4(a), 5(a)(1)). Note, this includes practices disclosed in the notices that exceed regulatory requirements; and
  - c. Include, and adequately describe, all required items of information and contain examples as applicable (§§6, 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 if the institution has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
  - a. Timeliness of delivery (§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) (§9).
  - c. For customers only, review the timeliness of delivery (§§4(d), 4(e), and 5(a)), means of delivery of annual notice §9(c)), and accessibility of or ability to retain the notice (§9(e)).

**C. Checklist Cross References—Module 2**

<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
14, 15	Exceptions	48, 49, 50