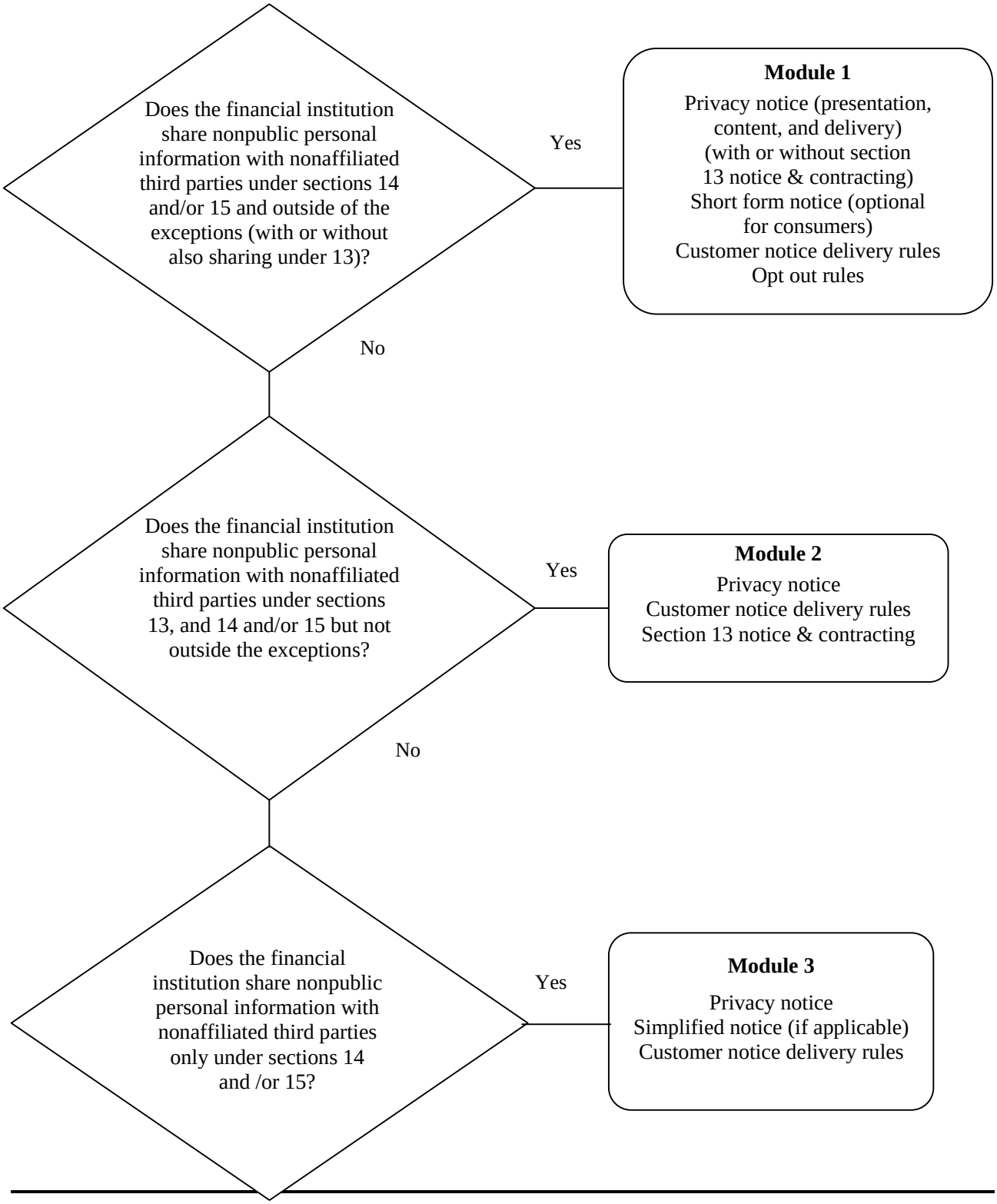
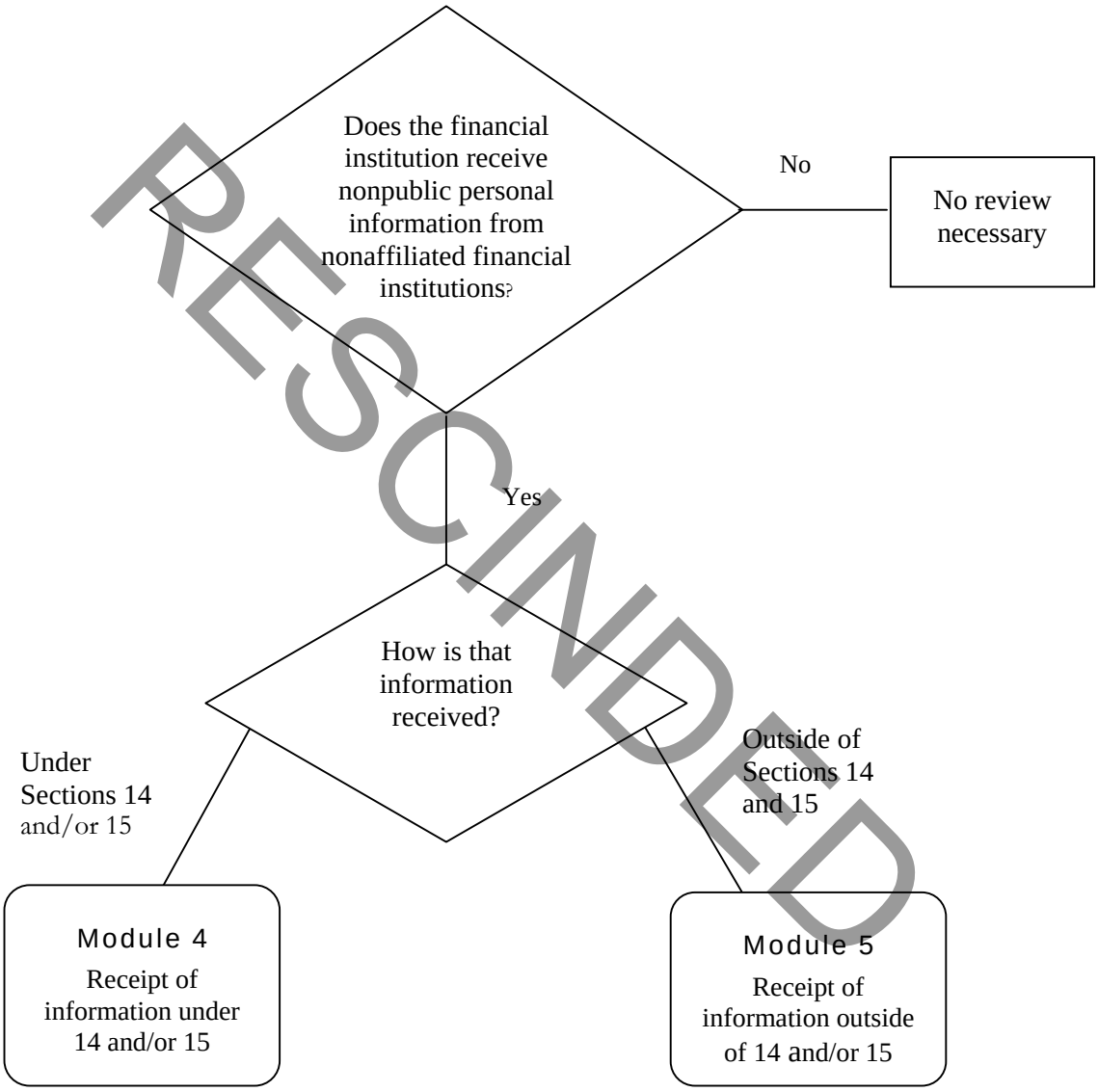
RESCINDED

This document and any attachments are superseded by Comptroller's Handbook - Consumer Compliance - Privacy of Consumer Financial Information.

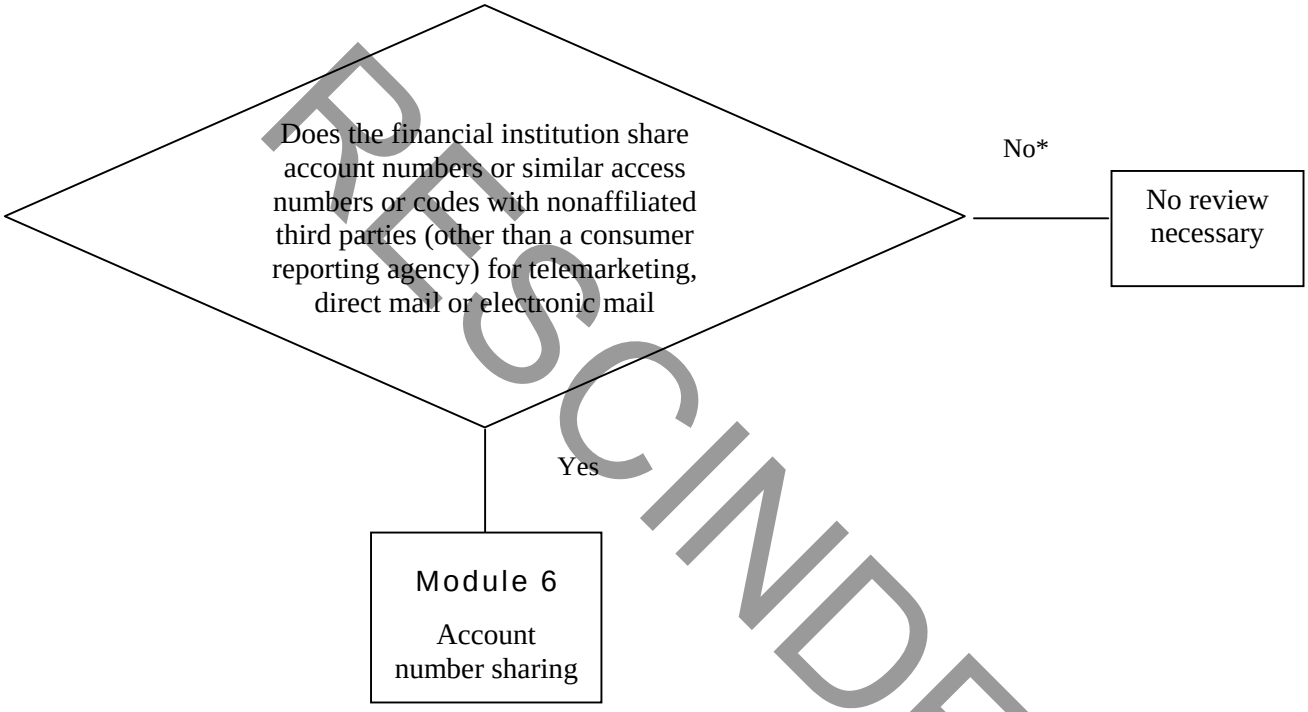
PRI REE



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 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));

   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

   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);

   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)); 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 (§7(e), (f), (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

An institution may approach sharing consumer information with nonaffiliates differently with respect to customers versus noncustomers. Determine whether the thrift has adopted different policies along these lines. When sharing consumer information with nonaffiliates beyond the exceptions, thrifts have different obligations depending on whether the consumer is a customer or not. Use this table to determine whether the institution has established the requisite policies, systems and controls with respect to its obligations to both categories of consumers. Please note that, in the interest of brevity, this table presents the most commonly anticipated issues and offers concise reference sources; in applying it to complex situations encountered during the course of the examination, please read it in conjunction with the rule text.

CUSTOMER	SUBJECT	NONCUSTOMER
How does the thrift properly identify those persons/accounts that constitute customers? Do they meet regulatory standards? Are there system controls for confirming or testing results?	**Verification of Distinction Between Customer and Noncustomer.**	How does the thrift categorize those persons/transactions that are treated as non-customers? Do they meet regulatory standards? Are there system controls for confirming or testing categorizations?
Short Form Notice is not available. Content required is covered in Checklist Items 8, 9, 10, 11, 20, 21, 22.	**Initial Notice Content (including opt out information.).**	Short Form Notice is available. Checklist Item 16
Must be executed such that each customer can "reasonably expect" to receive "actual notice" (in written or electronic form) Checklist Items 35, 36 Must be presented in a "clear and conspicuous" manner Checklist Items 1, 3	**Initial Notice Delivery***	The initiation of a transaction is the first opportunity for the thrift to provide notice to a noncustomer consumer. At that point, the same considerations of "reasonableness of delivery method" and "clear and conspicuous" display must be met. Checklist Item 2 For an Isolated Transaction: "Reasonable Oppty" can be interpreted as the consumer's opt out decision, as a necessary part of proceeding with the transaction [12 CFR 573.9(b)(1)(iv)]
Not later than when a customer relationship is established (earlier timing also permissible) Checklist Items 1, 3	**Initial Notice Timing**	Before any NPI is disclosed outside the exceptions; "reasonable oppty to opt out" must be factored into timeframe Checklist Item 2
Two narrow circumstances: (1) Customer relationship is not created by the individual's election; (2) Where, to do otherwise, would result in a substantial delay of service to the customer **and** the customer agrees to later notice receipt Checklist Items 4, 5	**Delayed Initial Notice**	Not available

CUSTOMER	SUBJECT	NONCUSTOMER
"Reasonable" is defined as: *for mailed notice* – within 30 days of date mailed *for electronic notice* – within 30 days of electronic acknowledgement of notice receipt Checklist Item 42	**Reasonable Opportunity to Exercise Opt Out**	For an Isolated Transaction: "Reasonable Oppty" can be interpreted as the consumer's opt out decision, as a necessary part of proceeding with the transaction [12 CFR 573.9(b)(1)(iv)]
A "clear and conspicuous" notice, that "accurately reflects privacy policies and practices" of the institution Checklist Items 6, 8, 9, 10, 11, 12, 14	**Annual Notice Content**	Not Applicable
Must be executed such that each customer can "reasonably expect" to receive "actual notice" (in written or electronic form) Checklist Items 35, 36, 37 Must be presented in a "clear and conspicuous" manner Checklist Items 1, 3	**Annual Notice Delivery**	Not Applicable
Must be provided "not less than annually during the continuation of the customer relationship" Checklist Item 6	**Annual Notice Timing**	Not Applicable
Only necessary when changes to privacy practices invoke an opt out right not previously provided Checklist Item 33	**Revised Notice Trigger**	Not Applicable (presumably, the most recent notice will always be provided to a noncustomer consumer who is entitled to receive a privacy notice)
4 elements: (1) explanation of privacy policies and practices (2) new opt out notice (or inclusion of opt out language) (3) reasonable oppty to opt out (4) customer does not opt out Checklist Item 33	**Revised Notice Content**	Not Applicable

CUSTOMER	SUBJECT	NONCUSTOMER
Must be executed such that each customer can "reasonably expect" to receive "actual notice" (in written or electronic form) Checklist Items 34, 35, 36 Must be presented in a "clear and conspicuous" manner Checklist Items 1, 3	**Revised Notice Delivery and Timing**	Not Applicable
Institution must provide notice(s) in a form such that customer can retain or obtain later in writing Checklist Item 38, 39	**All Types of Notices: Retention and Subsequent Accessibility**	Not Applicable
Do the thrift's systems operate to effectively process customer opt out choices? a. Must comply w/ opt out direction "as soon as reasonably practicable upon receipt" Checklist Item 29 b. Are opt out choices for joint acct holders clearly explained and executed as described in the notice? Checklist Items 24, 25, 26, 27, 28 c. Opt out right available at any time? Checklist Item 30 d. Opt out direction honored until revoked in writing? Checklist Item 31	**Opt Out Followed?** **a. Timeliness** **b. Joint Customers** **c. Continuous Availability of Right** **d. Revocation**	Do the thrift's systems operate to effectively process noncustomer opt out choices? (items a and b) Checklist Items 24 - 29

*** Note to Examiners:**

The Privacy Regulation, with an effective date of November 13, 2000 but a delayed mandatory compliance date of July 1, 2001, will present some unique implementation challenges. There will necessarily be a transition period as financial institutions evaluate current information sharing practices and choose either to maintain or revise them post July 1st. The following is a brief summary of some issues that may be applicable at the particular institution under review:

- Initial Notice – For all individuals who are existing customers of the institution prior to July 1, 2001, the bank must provide an Initial Notice which describes its privacy policies and practices as they will exist on and after July 1, 2001. The notice may be purely prospective in nature or the bank may have already commenced operating pursuant to the terms of the notice. The purpose of this "one-time only" distribution to existing customers is to communicate how the institution will implement the Privacy Regulation and to allow an opt out opportunity, if applicable.

  As of July 1, 2001 and beyond, the Initial Notice "concept" will generally be paired with new customers to the bank. Typically, the Initial Notice will be given to the new customer in the course of opening a deposit account, contracting for safety deposit box service, conducting a loan transaction or any of the other varied methods in which a customer relationship is established. Over time, the distinction between customers pre-July 1, 2001 and those who become customers after that date will be eliminated entirely. The importance during the transition phase is to ensure that the former group has received notice sufficiently prior to the July 1st date to allow for a reasonable opt out period.

- Former Customers – The regulation establishes a level of protection for former, as well as current, customers of the institution. A "former customer" is defined in the regulation [§573.5(b)(2)(i-iii)] through the use of examples, separately delineating deposit account, closed-end loan and credit card customers. Additionally, a former customer is also defined as someone with whom the institution has not communicated over the last 12 months, subject to some exceptions [§573.5(b)(2)(iv)].

  During the transition period, it will be important to evaluate the institution's plans to disclose NPI of former customers, opt out implications, notice delivery and implementation of customer directions. The earliest privacy examination reviews will necessarily be focusing on former customers whose relationship terminated prior to July 1, 2001. However, there will be a consistent place in the examination scope for the evaluation of the institution's treatment of former customers, as there will be a regular flow of new and departing customers.

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));

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

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

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

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 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 (§§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 (§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 (§§4(a), 4(d), 4(e), 5(a)); and

   b. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the customer agrees; or as a necessary step of a transaction) (§9) and accessibility of or ability to retain the notice (§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 & 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 (§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 b below (§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 (§11(a)(1)(iii)).

C. Checklist Cross References

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

Rediscloure 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 (§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 (§§10, 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).

B. Obtain and review a sample of contracts with agents or service providers to whom the financial institution discloses account numbers for use in connection with marketing the institution's own products or services. Determine whether the institution shares account numbers with nonaffiliated third parties only to perform marketing for the institution's own products and services. Ensure that the contracts do not authorize these nonaffiliated third parties to directly initiate charges to customer's accounts (§12(b)(1)).

C. Obtain a sample of materials and information provided to the consumer upon entering a private label or affinity credit card program. Determine if the participants in each program are identified to the customer when the customer enters into the program (§12(b)(2)).

D. Checklist Cross References

Regulation Section	Subject	Checklist Question
12	Account number sharing	46