

NCUA LETTER TO CREDIT UNIONS

**NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA**

DATE: February 2002 **LETTER NO.:** 02-CU-02

TO: All Federally Insured Credit Unions

SUBJ: NCUA's Privacy of Consumer Financial Information Examination Program

ENCL: 1) Privacy of Consumer Financial Information
2) Questionnaire - Privacy of Consumer Financial Information

Dear Board Of Directors:

NCUA's recent Letter to Credit Unions 01-CU-02 provided information about requirements relating to consumer financial privacy to assist credit unions in complying with Title V, Section 502, Subtitle A of the Gramm-Leach-Bliley Act (the "Act"). The purpose of this letter is to provide additional information regarding the NCUA examination procedures to assist in complying with the Act.

Examination procedure requires the completion of the enclosed questionnaire, "Privacy of Consumer Financial Information." This questionnaire includes, in summary format, key areas of review.

For your reference, I am also enclosing documentation adapted from Federal Financial Institutions Examination Council (FFIEC) guidelines. This documentation includes an introduction to Privacy of Consumer Financial Information, as well as examination procedures, a flowchart, and an examination checklist.

Sincerely,

/S/

Dennis Dollar
Chairman

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 May 18, 2000, the National Credit Union Administration (NCUA) published 12 C.F.R. Part 716 implementing provisions of the Act governing the privacy of consumer financial information. The regulation establishes rules governing duties of a credit union 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 credit union 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 §716.13, §716.14 or §716.15 of the regulations.
- ◆ Regardless of whether a credit union shares nonpublic personal information, the credit union must provide notices of its privacy policies to its members.
- ◆ A credit union generally may not disclose member account numbers to any nonaffiliated third party for marketing purposes.
- ◆ A credit union must follow reuse and redisclosure limitations on any nonpublic personal information it receives from a nonaffiliated financial institution.

The privacy regulation 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 regulation, a number of key concepts are used. These concepts include “financial institution”; “nonpublic personal information”; “nonaffiliated third party”; the “opt out” right and the exceptions to that right; and “consumer” and “member.” Each concept is briefly discussed below. A more complete explanation of each appears in the regulation.

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, credit unions, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents.¹

Nonpublic Personal Information:

“Nonpublic personal information” generally is any information that is not publicly available and that:

- a consumer provides to a credit union to obtain a financial product or service from the credit union;
- results from a transaction between the consumer and the credit union involving a financial product or service; or
- a credit union otherwise obtains about a consumer in connection with providing a financial product or service.

Information is publicly available if a credit union has a reasonable basis to believe that the information is lawfully made available to the general public from government records, widely distributed media, or legally required disclosures to the general public. Examples include information in a 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).

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 credit union’s members 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 is a member of the credit union, which is not publicly available information.

¹ Certain functionally-regulated credit union service organizations (CUSOs), 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.

However, if the credit union has a reasonable basis to believe that certain member relationships are a matter of public record, then any list of these relationships would be considered publicly available information. For instance, a list of members with mortgages where the mortgages are recorded in public records would be considered publicly available information. The credit union could provide a list of such members, and include on that list any other publicly available information it has about the members on that list without having to provide notice or opt out.

Nonaffiliated Third Party:

A “nonaffiliated third party” is any person except a credit union’s affiliate or a person employed jointly by a credit union and a company that is not the credit union’s affiliate. An “affiliate” of a credit union is any company that controls, is controlled by, or is under common control with the credit union. For federal credit unions, a credit union service organization (CUSO) that is controlled by the credit union would constitute the only affiliate. NCUA will presume a credit union has a controlling influence if the CUSO is 67 percent owned by that credit union or by that credit union and other credit unions.

Opt Out Right and Exceptions:**The Right**

Consumers must be given the right to “opt out” of, or prevent, a credit union from disclosing nonpublic personal information about them to a nonaffiliated third party, unless an exception to that right applies. The exceptions are detailed in §716.13, §716.14 or §716.15 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 provided a reasonable amount of time to exercise the opt out right. For example, it would be reasonable if the credit union allows 30 days from the date of mailing a notice or 30 days after member 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 §716.13, §716.14 or §716.15 of the regulations. Credit unions 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 credit union or to function on its behalf, including marketing the credit union's own products or services or those offered jointly by the credit union and another financial institution. The exception is permitted only if the credit union 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 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 §716.14 or §716.15 (discussed below), the credit union does not have to comply with the additional disclosure and confidentiality requirements of §716.13. Disclosure under this exception could include the outsourcing of marketing to an advertising company. (12 C.F.R. §716.14)
- ◆ 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 members. 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. (12 C.F.R. §716.14)
- ◆ For specified other disclosures that a credit union normally makes, such as to protect against or prevent actual or potential fraud; to the credit union's attorneys, accountants, and auditors; or to comply with applicable legal requirements, such as the disclosure of information to regulators. (12 C.F.R. §716.15)

Consumer and Member:

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

A "consumer" is an individual, or that individual's legal representative, who obtains or has obtained a financial product or service from a credit union that is to be used primarily for personal, family, or household purposes.

A "financial service" includes, among other things, a credit union's evaluation or brokerage of information that the credit union collects in connection with a request or an application from a consumer for a financial product or service. For example, a financial service includes an evaluation of an application for membership, even if the application is ultimately rejected or withdrawn.

Consumers who are not members are entitled to an initial privacy and opt out notice only if the credit union wants to share their nonpublic personal information with nonaffiliated third parties outside of the exceptions.

A “member” is a consumer who has a “member relationship” with a credit union. A “member relationship” is a *continuing* relationship between a consumer and a credit union under which the credit union provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

For the purposes of the privacy regulation, the term member will include certain nonmembers. For example, the following are considered members:

- An individual who meets the definition of member, as defined in the credit union’s bylaws;
- A nonmember who has a share, share draft, or credit card account held jointly with a member;
- A nonmember who has a loan that the credit union services;
- A nonmember who has an account in a low-income credit union; and
- A nonmember who has an account in a federally insured state-chartered credit union pursuant to state law.

Members are entitled to initial and annual privacy notices regardless of the information disclosure practices of their credit union.

There is a special rule for loans. When a member obtains a loan from a credit union, and that is the only basis for the member relationship, if the credit union subsequently transfers the servicing rights to that loan to another financial institution, the member relationship transfers with the servicing rights. However, any information on the borrower retained by the credit union selling 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 member. For example, if an individual purchases a traveler’s check from a credit union where the person has no account, the individual will be a consumer but not a member of that credit union because he or she has not established a member relationship. Likewise, if an individual uses the ATM of a credit union where the individual has no account, even repeatedly, the individual will be a consumer, but not a member of that credit union.

Credit Union Duties

The regulation establishes specific duties and limitations for a credit union based on its activities. Credit unions that intend to disclose nonpublic personal information outside the exceptions will have to provide opt out rights to their members and to consumers who are not members. All credit unions have an obligation to provide an initial and annual notice of their privacy policies to their members. All credit unions 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 credit union duties and limitations appears below. A more complete explanation of each appears in the regulations.

Notice and Opt Out Duties to Consumers:

If a credit union intends to disclose nonpublic personal information about any of its consumers (whether or not they are members) to a nonaffiliated third party, and an exception does not apply, then the credit union 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 credit union discloses the information to the nonaffiliated third party, to opt out.

The credit union 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 credit union must provide a *revised notice* before the credit union 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 credit union need not comply with the initial and opt-out notice requirements for consumers who are not members if the credit union limits disclosure of nonpublic personal information to the exceptions.

Special Rule for Loans. A credit union must provide an initial notice to a co-borrower or guarantor on a loan, who has no other member relationship with the credit union, if it shares his or her nonpublic personal information with nonaffiliated third parties other than as allowed under the exceptions. Annual notices may be provided to the co-borrowers and guarantors jointly.

Notice Duties to Members:

In addition to the duties described above, there are several duties unique to members. In particular, regardless of whether the credit union discloses or intends to disclose nonpublic personal information, a credit union must provide notice to its members of its privacy policies and practices at various times.

- A credit union must provide an *initial notice* of its privacy policies and practices to each member, not later than the time a member relationship is established. Section 4(e) of the regulation describes the exceptional cases in which delivery of the notice is allowed subsequent to the establishment of the member relationship.
- A credit union must provide an *annual notice* at least once in any period of 12 consecutive months during the continuation of the member relationship.
- Generally, new privacy notices are not required for each new product or service. However, a credit union must provide a *new notice* to an existing member when the member obtains a new financial product or service from the credit union, if the initial or annual notice most recently provided to the member was not accurate with respect to the new financial product or service.
- When a credit union does not disclose nonpublic personal information (other than as permitted under §716.14 or §716.15) and does not reserve the right to do so, the credit union 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 credit union's privacy practices.

Delivery Rules. Privacy notices must be provided so that each recipient can reasonably be expected to receive the actual notice in writing or, if the consumer agrees, electronically. To meet this standard, a credit union could, for example, (1) hand-deliver a printed copy of the notice to its consumer, (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 credit union's Web site and require the consumer to acknowledge receipt of the notice as a necessary step to completing the transaction.

For members only, a credit union must provide the initial notice (as well as the annual notice and any revised notice) so that a member may be able to retain or subsequently access the notice. A written notice satisfies this requirement. For members who obtain financial products or services electronically, and agree to receive their notices on the credit union's Web site, the credit union may provide the current version of its privacy notice on its Web site.

Notice Content. A privacy notice must contain specific disclosures. However, a credit union may provide to consumers who are not members a "short form" initial notice together with an opt out notice stating that the credit union'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 credit unions must provide in their privacy notices, as applicable:

- (1) categories of information collected;
- (2) categories of information disclosed;
- (3) categories of affiliates and nonaffiliated third parties to whom the credit union may disclose information;
- (4) policies with respect to the treatment of former members' information;
- (5) information disclosed to service providers and joint marketers (§716.13);
- (6) an explanation of the opt out right and methods for opting out;
- (7) any opt out notices the credit union must provide under the Fair Credit Reporting Act with respect to affiliate information sharing;
- (8) policies for protecting the security and confidentiality of information; and
- (9) a statement that the credit union makes disclosures to other nonaffiliated third parties as permitted by law under §716.14 and §716.15.

Limitations on Disclosure of Account Numbers:

A credit union must not disclose an account number or similar form of access number or access code for a credit card, share, 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 credit union to its agent to market the credit union's own products or services (although the credit union must not authorize the agent to directly initiate charges to the member's account). Also not barred are disclosures to participants in private-label or affinity card programs, where the participants are identified to the member when the member enters the program.

Redisclosure and Reuse Limitations on Nonpublic Personal Information Received:

If a credit union receives nonpublic personal information from a nonaffiliated financial institution, the credit union's disclosure and use of the information is limited.

- ◆ For nonpublic personal information received under a §716.14 or §716.15 exception, the credit union is limited to:
 - Disclosing the information to the affiliates of the financial institution from which it received the information;
 - Disclosing the information to its own affiliates, who may, in turn, disclose and use the information only to the extent that the credit union can do so; and
 - Disclosing and using the information pursuant to a §716.14 or §716.15 exception (for example, a credit union receiving information for account processing could disclose the information to its auditors).

- ◆ For nonpublic personal information received other than under a §716.14 or §716.15 exception, the credit union'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;
 - Disclosing the information to its own affiliates, who may, in turn, disclose the information only to the extent that the credit union 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, a credit union

that received a member list from another credit union could disclose the list (1) in accordance with the privacy policy of the credit union that provided the list, (2) subject to any opt out election or revocation by the members on the list, and (3) in accordance with appropriate exceptions under §716.14 and §716.15.

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 credit union has entered into, on or before July 1, 2000, with a nonaffiliated third party to perform services for the credit union or functions on its behalf, as described in §716.13, will satisfy the confidentiality requirements of §716.13(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 Member Information

The regulations require a credit union to disclose its policies and practices for protecting the confidentiality, security, and integrity of nonpublic personal information about consumers (whether or not they are members). 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 credit union has security practices and procedures in place to ensure the confidentiality of the information in accordance with the credit union's policies.

NCUA has published guidelines (Appendix A to 12 C.F.R. Part 748 of the Rules and Regulations), pursuant to section 501(b) of the Gramm Leach Bliley Act, that address steps a credit union may take in order to protect member information. The guidelines relate only to information about members, rather than all consumers.

1. To assess the quality of a credit union's compliance management policies and procedures for implementing the privacy regulation, specifically ensuring consistency between what the credit union 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 credit union's internal controls and procedures for monitoring compliance with the privacy regulation.
3. To determine a credit union's compliance with the privacy regulation, specifically in meeting the following requirements:
 - Providing to consumers notices of its privacy policies and practices that are timely, accurate, clear and conspicuous, and delivered so that each consumer 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.
 - A. Through discussions with management and review of available information, identify the credit union'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:
 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);

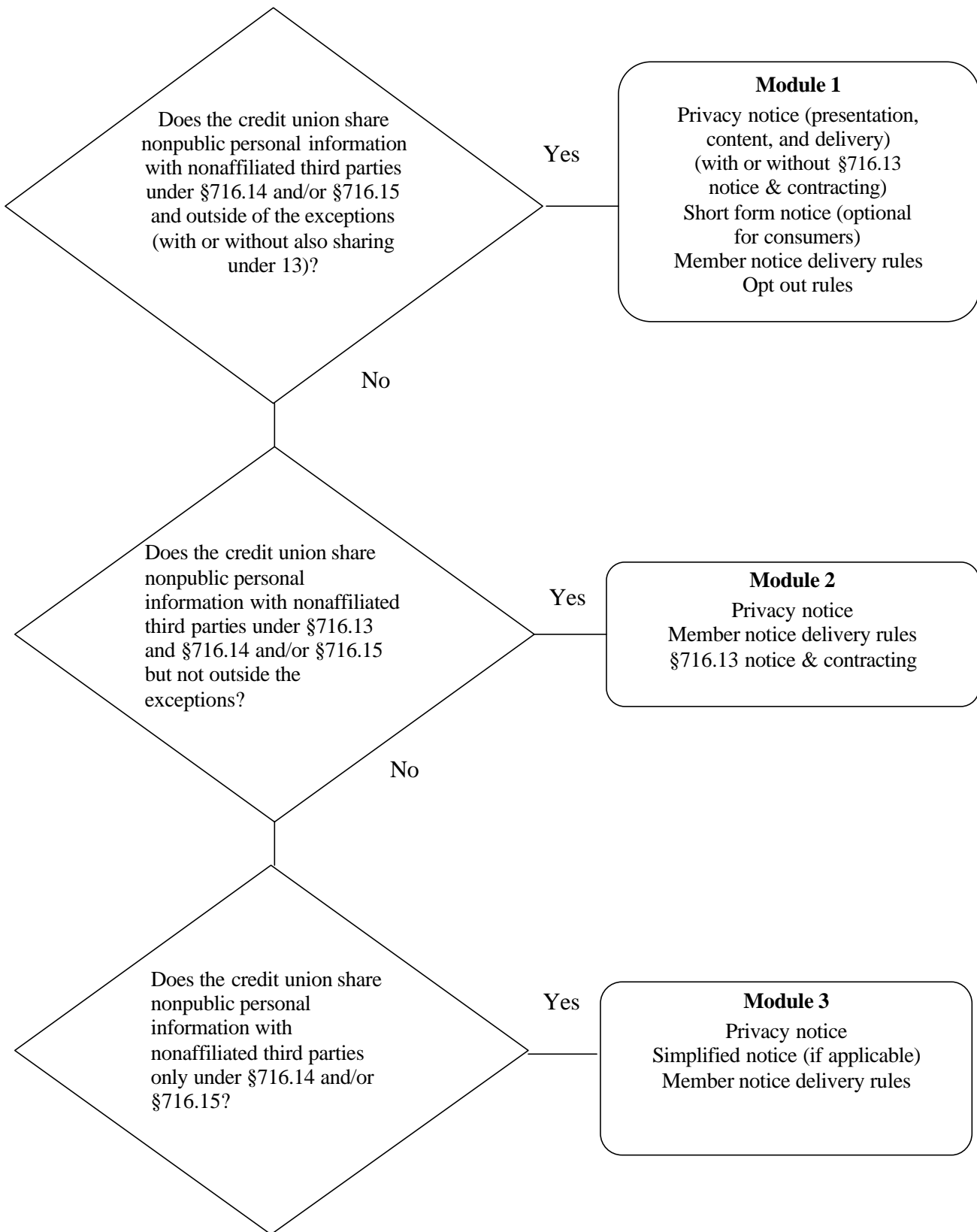
- prevent the unlawful disclosure and use of the information received from nonaffiliated financial institutions; and
 - prevent the unlawful disclosure of account numbers;
3. Information sharing agreements between the credit union and affiliates and service agreements or contracts between the credit union 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 §716.13 are met and whether the credit union is disclosing account number information in violation of §716.12);
 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 membership, loan, or investment products; for an over-the-counter purchase of a traveler's 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 credit union's categorization of its information sharing practices under §716.13, §716.14, §716.15, and outside of these exceptions.
 9. Results of an information systems inspection (used to determine the accuracy of the credit union'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 Rediscovery and Account Number Sharing Decision Trees, as necessary (Attachments B & C). Identify which module is applicable.
 - D. Determine the adequacy of the credit union'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 credit union'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 credit union'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 credit union's sharing practices (especially those within §716.13 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 credit union's compliance management system and level of risk identified. Each module contains a series of general instructions 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.

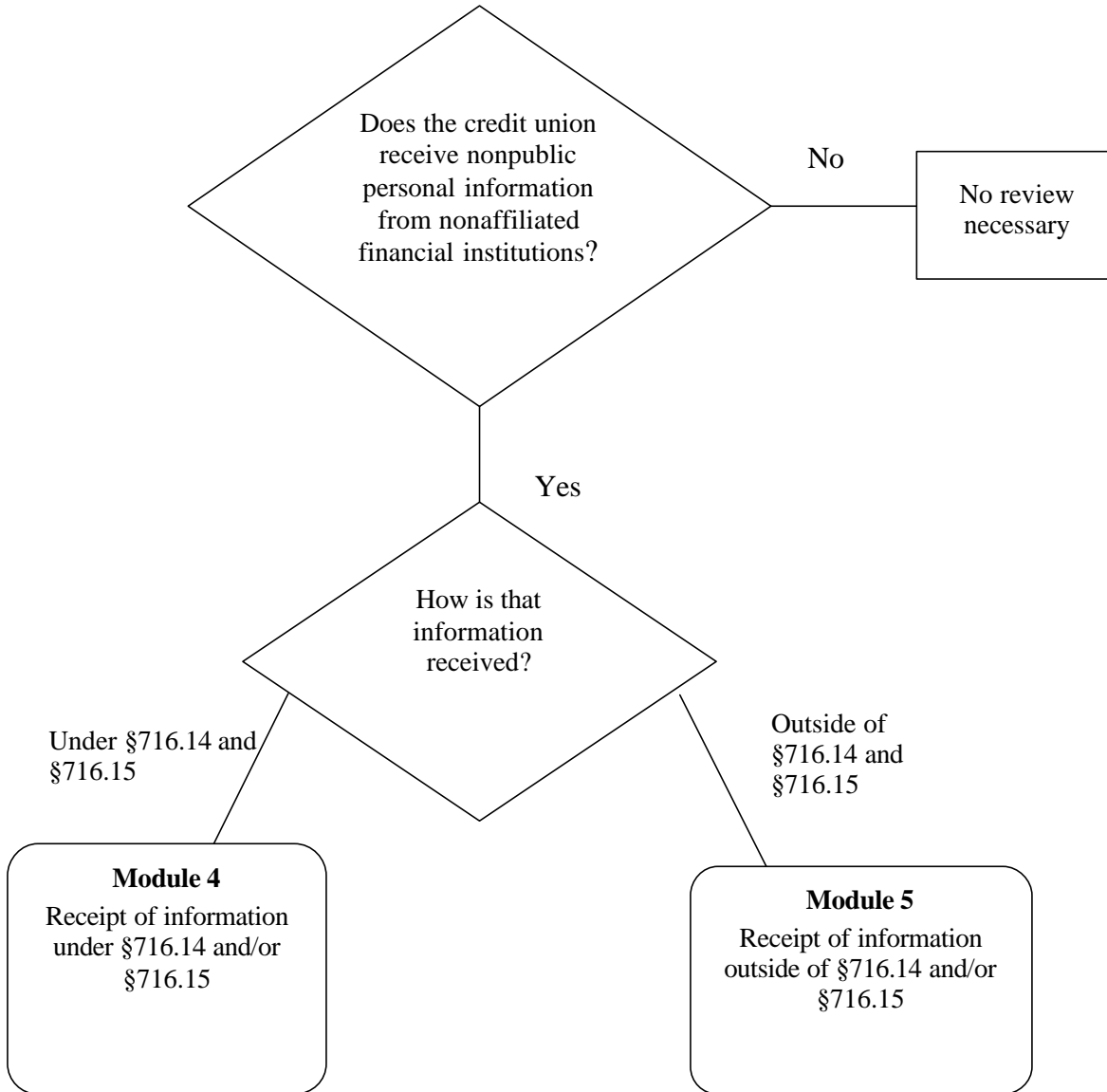
H. Formulate conclusions.

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 credit union's compliance system, as appropriate.
4. Discuss findings with management and obtain a commitment for corrective action.

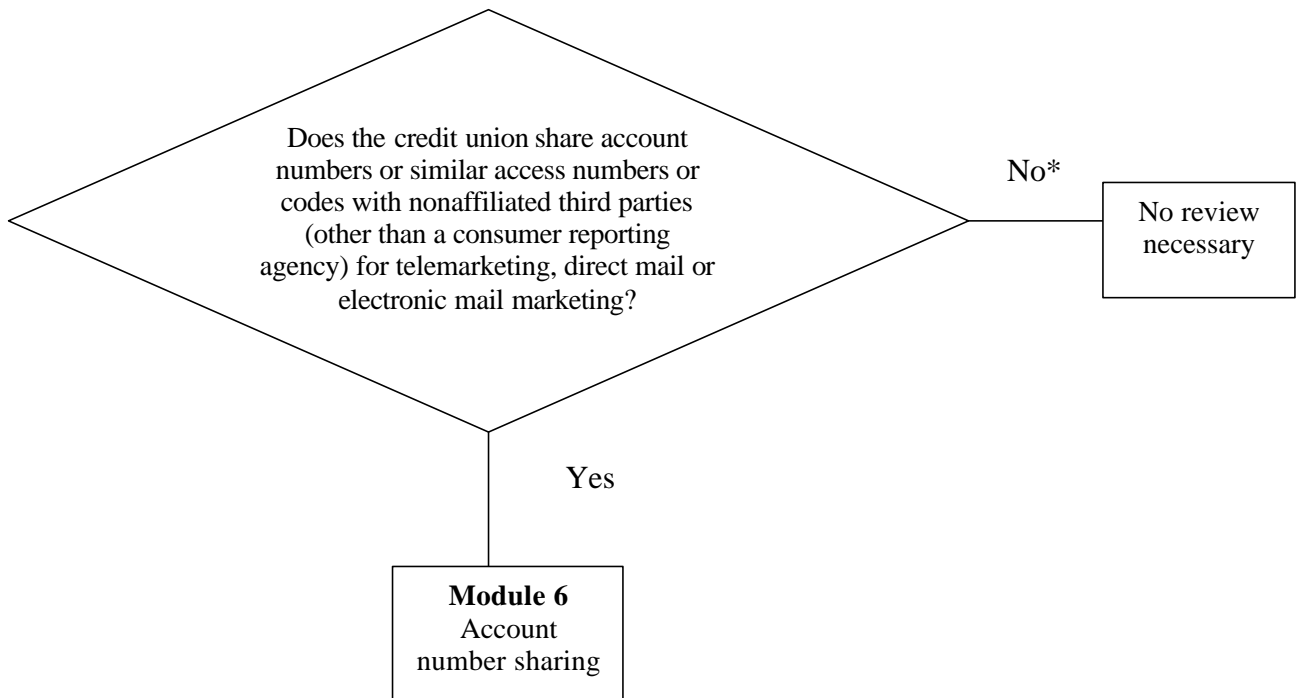
PRIVACY NOTICE AND OPT OUT DECISION TREE



**REUSE & REDISCLOSURE OF NONPUBLIC PERSONAL INFORMATION
RECEIVED FROM NONAFFILIATED FINANCIAL INSTITUTIONS DECISION TREE
(§716.s 11(a) and 11(b))**



**ACCOUNT NUMBER SHARING DECISION TREE
(§716.12)**



* This may include sharing of encrypted account numbers but not the decryption key.

Sharing nonpublic personal information with nonaffiliated third parties under §716.14 or §716.15 and outside of the exceptions (with or without also sharing under §716.13).

Note: Credit unions whose practices fall within this category engage in the most expansive degree of information sharing permissible. Consequently, these credit unions 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 credit union 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 credit union'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 credit union tells consumers (members and those who are not members) in its notices about its policies and practices in this regard and what the credit union actually does are consistent (§716.10, §716.6).
 - 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 (members and those who are not members) who chose not to opt out is shared (§716.10).
2. If the credit union also shares information under §716.13, obtain and review contracts with nonaffiliated third parties that perform services for the credit union not covered by the exceptions in §716.14 or §716.15. 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 §716.18 apply to certain of these contracts (§716.13(a)).

B. Presentation, Content, and Delivery of Privacy Notices

1. Review the credit union's initial, annual, and revised notices, as well as any short-form notices it may use for consumers who are not members. Determine whether or not these notices:
 - a. Are clear and conspicuous (§716.3(b), §716.4(a), §716.5(a)(1), §716.8(a)(1));

- b. Accurately reflect the policies and practices used by the credit union (§716.4(a), §716.5(a)(1), §716.8(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 (§716.6). Note that if the credit union shares under §716.13, the notice provisions for that section shall also apply.
 2. Through discussions with management, review of the credit union's policies and procedures, and a sample of electronic or written consumer records where available, determine if the credit union has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
 - a. Timeliness of delivery (§716.4(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) (§716.9); and
 - c. For members only, review the timeliness of delivery (§716.4(d), §716.4(e), §716.5(a)), means of delivery of annual notice (§716.9(c)), and accessibility of or ability to retain the notice (§716.9(e)).

C. Opt Out Right

1. Review the credit union's opt out notices. An opt out notice may be combined with the credit union's privacy notices. Regardless, determine whether the opt out notices:
 - a. Are clear and conspicuous (§716.3(b) and §716.7(a)(1));
 - b. Accurately explain the right to opt out (§716.7(a)(1));
 - c. Include and adequately describe the three required items of information (the credit union's policy regarding disclosure of nonpublic personal information, the consumer's opt out right, and the means to opt out) (§716.7(a)(1)); and
 - d. Describe how the credit union treats joint consumers (members and those who are not members), as applicable (§716.7(d)).
2. Through discussions with management, review of the credit union's policies and procedures, and a sample of electronic or written records where available, determine if the credit union has adequate procedures in place to provide the opt

out notice and comply with opt out directions of consumers (members and those who are not members), as appropriate. Assess the following:

- a. Timeliness of delivery (§716.10(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) (§716.9);
- c. Reasonableness of the opportunity to opt out (the time allowed to and the means by which the consumer may opt out) (§716.10(a)(1)(iii), §716.10(a)(3)); and
- d. Adequacy of procedures to implement and track the status of a consumer's (members and those who are not members) opt out direction, including those of former members (§716.7(e), (f), (g)).

D. Checklist Cross References

Regulation Section	Subject	Checklist Questions
§716.4(a); §716.6(a, b, d, e); and §716.9(a, b, g)	Privacy notices (presentation, content, and delivery)	2, 8-11, 14, 18, 35, 36, 40
§716.4(a, c, d, e); §716.5; and §716.9(c, e)	Member notice delivery rules	1, 3-7, 37, 38
§716.13	§716.13 notice and contracting rules (as applicable)	12, 47
§716.6(c)	Short form notice rules (optional for consumers only)	15-17
§716.7; §716.8; and §716.10	Opt out rules	19-34, 41-43
§716.14, §716.15	Exceptions	48, 49, 50

Sharing nonpublic personal information with nonaffiliated third parties under §716.13, and §716.14 and/or §716.15 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 credit union 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 credit union's compliance with disclosure limitations.
 - a. Compare the data shared and with whom the data was shared to ensure that the credit union accurately categorized its information sharing practices and is not sharing nonpublic personal information outside the exceptions (§716.13, §716.14, §716.15).
 - b. Compare the categories of data shared and with whom the data was shared to those stated in the privacy notice and verify that what the credit union tells consumers in its notices about its policies and practices in this regard and what the credit union actually does are consistent (§716.10, §716.6).
2. Review contracts with nonaffiliated third parties that perform services for the credit union not covered by the exceptions in §716.14 or §716.15. 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 §716.18 apply to certain of these contracts (§716.13(a)).

B. Presentation, Content, and Delivery of Privacy Notices

1. Review the credit union's initial and annual privacy notices. Determine whether or not they:
 - a. Are clear and conspicuous (§716.3(b), §716.4(a), §716.5(a)(1));
 - b. Accurately reflect the policies and practices used by the credit union (§716.4(a), §716.5(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 (§716.6, §716.13).

2. Through discussions with management, review of the credit union’s policies and procedures, and a sample of electronic or written consumer records where available, determine if the credit union has adequate procedures in place to provide notices to consumers, as appropriate. Assess the following:
 - a. Timeliness of delivery (§716.4(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) (§716.9); and
 - c. For members only, review the timeliness of delivery (§716.4(d), §716.4(e), and §716.5(a)), means of delivery of annual notice §716.9(c)), and accessibility of or ability to retain the notice (§716.9(e)).

C. Checklist Cross References

Regulation Section	Subject	Checklist Questions
§716.4(a); §716.6(a, b, d, e); and §716.9(a, b, g)	Privacy notices (presentation, content, and delivery)	2, 8-11, 14, 18, 35, 36, 40
§716.13	§716.13 notice and contracting rules	12, 47
(§716.4(a, c, d, e); §716.5; and §716.9(c, e))	Member notice delivery rules	1, 3-7, 37, 38
§716.14, §716.15	Exceptions	48, 49, 50

Sharing nonpublic personal information with nonaffiliated third parties only under §716.14 and/or §716.15.

Note: This module applies only to members.

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 credit union and the third party. Compare the data shared and with whom the data was shared to ensure that the credit union 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 credit union's initial and annual notices, as well as any simplified notice it may use. Note that the credit union may only use the simplified notice when it does not also share nonpublic personal information with affiliates outside of §716.14 and §716.15 exceptions. Determine whether or not these notices:
 - a. Are clear and conspicuous (§716.3(b), §716.4(a), §716.5(a)(1));
 - b. Accurately reflect the policies and practices used by the credit union (§716.4(a), §716.5(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 (§716.6).
2. Through discussions with management, review of the credit union's policies and procedures, and a sample of electronic or written member records where available, determine if the credit union has adequate procedures in place to provide notices to members, as appropriate. Assess the following:
 - a. Timeliness of delivery (§716.4(a), §716.4(d), §716.4(e), §716.5(a)); and
 - b. Reasonableness of the method of delivery (e.g., by hand; by mail; electronically, if the member agrees; or as a necessary step of a transaction) (§716.9) and accessibility of or ability to retain the notice (§716.9(e)).

C. Checklist Cross References

Regulation Section	Subject	Checklist Questions
§716.6	Member notice content and presentation	8-11, 14, 18
§716.6(c)	Simplified notice content (optional)	13
§716.4(a, d, e); §716.5; and §716.9	Member notice delivery process	1, 3-7, 35-40
§716.14, §716.15	Exceptions	48, 49, 50

Reuse & Redisclosure of nonpublic personal information received from a nonaffiliated financial institution under §716.14 and/or §716.15.

- A. Through discussions with management and review of the credit union’s procedures, determine whether the credit union has adequate practices to prevent the unlawful redisclosure and reuse of the information where the credit union is the recipient of nonpublic personal information (§716.11(a)).
- B. Select a sample of data received from nonaffiliated financial institutions, to evaluate the credit union’s compliance with reuse and redisclosure limitations.
 - 1. Verify that the credit union’s redisclosure of the information was only to affiliates of the financial institution from which the information was obtained or to the credit union’s own affiliates, except as otherwise allowed in (§716.11(a)(1)(i) and (ii)).
 - 2. Verify that the credit union only uses and shares the data pursuant to an exception in §716.14 and §716.15 (§716.11(a)(1)(iii)).
- C. Checklist Cross References

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

Redisclosure of nonpublic personal information received from a nonaffiliated financial institution outside of §716.14 and §716.15.

- A. Through discussions with management and review of the credit union’s procedures, determine whether the credit union has adequate practices to prevent the unlawful redisclosure of the information where the credit union is the recipient of nonpublic personal information (§716.11(b)).
- B. Select a sample of data received from nonaffiliated financial institutions and shared with others to evaluate the credit union’s compliance with redisclosure limitations.
 - 1. Verify that the credit union’s redisclosure of the information was only to affiliates of the financial institution from which the information was obtained or to the credit union’s own affiliates, except as otherwise allowed in step 2 below (§716.11(b)(1)(i) and (ii)).
 - 2. If the credit union shares information with entities other than those under step 1 above, verify that the credit union’s information sharing practices conform to those in the nonaffiliated financial institution’s privacy notice (§716.11(b)(1)(iii)).
 - 3. Also, review the procedures used by the credit union to ensure that the information sharing reflects the opt out status of the consumers of the nonaffiliated financial institution (§716.10, §716.11(b)(1)(iii)).
- C. Checklist Cross References

Regulation Section	Subject	Checklist Question
§716.11(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 credit union’s members (§716.12).

- B. Obtain and review a sample of contracts with agents or service providers to whom the credit union discloses account numbers for use in connection with marketing the credit union’s own products or services. Determine whether the credit union shares account numbers with nonaffiliated third parties only to perform marketing for the credit union’s own products and services. Ensure that the contracts do not authorize these nonaffiliated third parties to directly initiate charges to members’ accounts (§716.12(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 member when the member enters into the program (§716.12(b)(2)).

- D. Checklist Cross References

Regulation Section	Subject	Checklist Question
§716.12	Account number sharing	46

<u>Yes</u>	<u>No</u>	
		<p>SUBPART A Initial Privacy Notice</p> <p>1. Does the credit union provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to <u>all members</u> not later than when the member relationship is established, other than as allowed in §716.4(a)(1)? <i>(Note: No notice is required if nonpublic personal information is disclosed to nonaffiliated third parties only under an exception in §716.14 and §716.15, and there is no member relationship. [§716.4(b)] With respect to credit relationships with nonmembers, a credit union establishes a member relationship when it originates a consumer loan. If the credit union subsequently sells the servicing rights to the loan to another financial institution, and the loan was the only basis for a member relationship, the member relationship transfers with the servicing rights. [§716.4(c)])</i></p> <p>2. Does the credit union provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to <u>consumers</u> who are not members before any nonpublic personal information about the consumer is disclosed to a nonaffiliated third party, other than under an exception in §716.14 or §716.15? [§716.4(a)(2)] <i>(Note: A credit union is required to provide an initial notice to a co-borrower or guarantor on a loan where the loan is the only basis for the member relationship if the credit union shares his or her nonpublic information with nonaffiliated third parties other than for purposes under the exceptions.)</i></p> <p>3. Does the credit union provide to <u>existing members</u>, who obtain a new financial product or service, an initial privacy notice that covers the member’s new financial product or service, if the most recent notice provided to the member was not accurate with respect to the new financial product or service? [§716.4(d)(1)]</p> <p>4. Does the credit union provide initial notice <u>after establishing a member relationship</u> only if: a) the member relationship is not established at the member’s election; [§716.4(e)(1)(i)] or b) to do otherwise would substantially delay the member’s transaction (e.g. in the case of a telephone application), and the member agrees to the subsequent delivery? [§716.4 (e)(1)(ii)]</p> <p>5. When the subsequent delivery of a privacy notice is permitted, does the credit union provide notice after establishing a member relationship within a reasonable time? [§716.4(e)]</p>

<u>Yes</u>	<u>No</u>	
		<p>Annual Privacy Notice</p> <p>6. Does the credit union 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 members, throughout the member relationship? [§716.5(a)(1)and (2)] <i>(Note: Annual notices are not required for former members. [§716.5(b)(1)and (2)])</i></p> <p>7. Does the credit union provide an annual privacy notice to each member whose loan the credit union owns the right to service? [§716.5(c), §716.4(c)(2)]</p> <p>Content of Privacy Notices</p> <p>8. Do the initial, annual, and revised privacy notices include each of the following, as applicable:</p> <ul style="list-style-type: none"> a. the categories of nonpublic personal information that the credit union collects; [§716.6(a)(1)] b. the categories of nonpublic personal information that the credit union discloses; [§716.6(a)(2)] c. the categories of affiliates and nonaffiliated third parties to whom the credit union discloses nonpublic personal information, other than parties to whom information is disclosed under an exception in §716.14 or §716.15; [§716.6(a)(3)] d. the categories of nonpublic personal information disclosed about former members, and the categories of affiliates and nonaffiliated third parties to whom the credit union discloses that information, other than those parties to whom the credit union discloses information under an exception in §716.14 or §716.15; [§716.6(a)(4)] e. if the credit union discloses nonpublic personal information to a nonaffiliated third party under §716.13, and no exception under §716.14 or §716.15 applies, a separate statement of the categories of information the credit union discloses and the categories of third parties with whom the credit union has contracted; [§716.6(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; [§716.6(a)(6)] g. any disclosures that the credit union makes under §603(d)(2)(A)(iii) of the Fair Credit Reporting Act (FCRA); [§716.6(a)(7)] h. the credit union’s policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; [§716.6(a)(8)] and
<u>Yes</u>	<u>No</u>	<ul style="list-style-type: none"> i. a general statement--with no specific reference to the exceptions or to the third parties--that the credit union makes disclosures to other nonaffiliated third parties as permitted by law? [§716.6(a)(9), (b)]

	<p><i>(Note: Sample clauses for these items appear in Appendix A of the Regulation.)</i></p> <p>9. Does the credit union list the following categories of nonpublic personal information that it collects, as applicable:</p> <ul style="list-style-type: none"> a. information from the consumer; [§716.6(e)(1)(i)] b. information about the consumer’s transactions with the credit union or its affiliates; [§716.6(e)(1)(ii)] c. information about the consumer’s transactions with nonaffiliated third parties; [§716.6(e)(1)(iii)] and d. information from a consumer reporting agency? [§716.6(e)(1)(iv)] <p>10. Does the credit union list the following categories of nonpublic personal information that it discloses, as applicable, and a few examples of each, or alternatively state that it reserves the right to disclose all the nonpublic personal information that it collects:</p> <ul style="list-style-type: none"> a. information from the consumer; b. information about the consumer’s transactions with the credit union or its affiliates; c. information about the consumer’s transactions with nonaffiliated third parties; and d. information from a consumer reporting agency? [§716.6(e)(2)] <p><i>(Note: Examples are recommended under §716.6(e)(2) although not under §716.6(e)(1).)</i></p> <p>11. Does the credit union list the following categories of affiliates and nonaffiliated third parties to whom it discloses information, as applicable, and a few examples to illustrate the types of the third parties in each category:</p> <ul style="list-style-type: none"> a. financial service providers; [§716.6(e)(3)(i)] b. non-financial companies; [§716.6(e)(3)(ii)] and c. others? [§716.6(e)(3)(iii)] <p>12. Does the credit union make the following disclosures regarding service providers and joint marketers to whom it discloses nonpublic personal information under §716.13:</p> <ul style="list-style-type: none"> a. as applicable, the same categories and examples of nonpublic personal information disclosed as described in paragraphs (a)(2) and (e)(2) of §716.6 (see questions 8b and 10); and [§716.6(e)(4)(i)] b. that the third party is a service provider that performs marketing on the credit union’s behalf or on behalf of the credit union and another financial institution; [§716.6(e)(4)(ii)(A)] or
<p><u>Yes</u></p>	<p><u>No</u></p> <ul style="list-style-type: none"> c. that the third party is a financial institution with which the credit union has a joint marketing agreement? [§716.6(e)(4)(ii)(B)] <p>13. If the credit union does not disclose nonpublic personal information, and does not reserve the right to do so, other than under exceptions in §716.14 and</p>

		<p>§716.15, does the credit union provide a simplified privacy notice that contains at a minimum:</p> <ul style="list-style-type: none"> a. a statement to this effect; b. the categories of nonpublic personal information it collects; c. the policies and practices the credit union uses to protect the confidentiality and security of nonpublic personal information; and d. a general statement that the credit union makes disclosures to other nonaffiliated third parties as permitted by law? [§716.6(e)(5)] <p><i>(Note: Use of this type of simplified notice is optional; a credit union may always use a full notice.)</i></p> <p>14. Does the credit union describe the following about its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information:</p> <ul style="list-style-type: none"> a. who is authorized to have access to the information; and [§716.6(e)(6)(i)] b. whether security practices and policies are in place to ensure the confidentiality of the information in accordance with the credit union’s policy? [§716.6(e)(6)(ii)] <p><i>(Note: The credit union is not required to describe technical information about the safeguards used in this respect.)</i></p> <p>15. If the credit union provides a short-form initial privacy notice with the opt out notice, does the credit union do so only to consumers with whom the credit union does not have a member relationship? [§716.6(c)(1)]</p> <p>16. If the credit union provides a short-form initial privacy notice according to §716.6(c)(1), does the short-form initial notice:</p> <ul style="list-style-type: none"> a. conform to the definition of “clear and conspicuous”; [§716.6(c)(2)(i)] b. state that the credit union’s full privacy notice is available upon request; [§716.6(c)(2)(ii)] and c. explain a reasonable means by which the consumer may obtain the notice? [§716.6(c)(2)(iii)] <p><i>(Note: The credit union is not required to deliver the full privacy notice with the short-form initial notice. [§716.6(c)(3)])</i></p> <p>17. Does the credit union provide consumers who receive the short-form initial notice with a reasonable means of obtaining the longer initial notice, such as:</p> <ul style="list-style-type: none"> a. a toll-free telephone number that the consumer may call to request the notice; [§716.6(c)(4)(i)] or
<u>Yes</u>	<u>No</u>	<ul style="list-style-type: none"> b. for the consumer who conducts business in person at the credit union’s office, having copies available to provide immediately by hand-delivery? [§716.6(c)(4)(ii)] <p>18. If the credit union, in its privacy policies, reserves the right to disclose nonpublic personal information to nonaffiliated third parties in the future, does the privacy</p>

		<p>notice include, as applicable, the:</p> <ul style="list-style-type: none"> a. categories of nonpublic personal information that the credit union reserves the right to disclose in the future, but does not currently disclose; [§716.6(d)(1)] and b. categories of affiliates or nonaffiliated third parties to whom the credit union reserves the right in the future to disclose, but to whom it does not currently disclose, nonpublic personal information? [§716.6(d)(2)] <p>Opt Out Notice</p> <p>19. If the credit union discloses nonpublic personal information about a consumer to a nonaffiliated third party, and the exceptions under §716.13-§716.15 do not apply, does the credit union provide the consumer with a clear and conspicuous opt out notice that accurately explains the right to opt out? [§716.7(a)(1)]</p> <p>20. Does the opt out notice state:</p> <ul style="list-style-type: none"> a. that the credit union discloses or reserves the right to disclose nonpublic personal information about the consumer to a nonaffiliated third party; [§716.7(a)(1)(i)] b. that the consumer has the right to opt out of that disclosure; [§716.7(a)(1)(ii)] and c. a reasonable means by which the consumer may opt out? [§716.7(a)(1)(iii)] <p>21. Does the credit union provide the consumer with the following information about the right to opt out:</p> <ul style="list-style-type: none"> a. all the categories of nonpublic personal information that the credit union discloses or reserves the right to disclose; [§716.7(a)(2)(i)(A)] b. all the categories of nonaffiliated third parties to whom the information is disclosed; [§716.7(a)(2)(i)(A)]; c. that the consumer has the right to opt out of the disclosure of that information; [§716.7(a)(2)(i)(A)] and d. the financial products or services that the consumer obtains to which the opt out direction would apply? [§716.7(a)(2)(i)(B)] <p>22. Does the credit union provide the consumer with at least one of the following reasonable means of opting out, or with another reasonable means:</p> <ul style="list-style-type: none"> a. check-off boxes prominently displayed on the relevant forms with the opt out notice; [§716.7(a)(2)(ii)(A)]
<u>Yes</u>	<u>No</u>	<ul style="list-style-type: none"> b. a reply form included with the opt out notice; [§716.7(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 credit union’s web site, if the consumer agrees to the electronic delivery of information; [§716.7(a)(2)(ii)(C)] or d. a toll-free telephone number? [§716.7(a)(2)(ii)(D)] <p><i>(Note: The credit union may require the consumer to use one specific means, as long as that means is reasonable for that consumer. [§716.7(a)(iv)])</i></p>

		<p>23. If the credit union delivers the opt out notice after the initial notice, does the credit union provide the initial notice once again with the opt out notice? [§716.7(c)]</p> <p>24. Does the credit union provide an opt out notice, explaining how it will treat opt out directions by the joint consumers, to at least one party in a joint consumer relationship? [§716.7(d)(1)]</p> <p>25. Does the credit union permit each of the joint consumers in a joint relationship to opt out? [§716.7(d)(2)]</p> <p>26. Does the opt out notice to joint consumers state that either:</p> <ul style="list-style-type: none"> a. the credit union will consider an opt out by a joint consumer as applying to all associated joint consumers; [§716.7(d)(2)(i)] or b. each joint consumer is permitted to opt out separately? [§716.7(d)(2)(ii)] <p>27. If each joint consumer may opt out separately, does the credit union permit:</p> <ul style="list-style-type: none"> a. one joint consumer to opt out on behalf of all of the joint consumers; [§716.7(d)(3)] b. the joint consumers to notify the credit union in a single response; [§716.7(d)(5)] and c. each joint consumer to opt out either for himself or herself, and/or for another joint consumer? [§716.7(d)(5)] <p>28. Does the credit union refrain from requiring all joint consumers to opt out before implementing any opt out direction with respect to the joint account? [§716.7(d)(4)]</p> <p>29. Does the credit union comply with a consumer's direction to opt out as soon as is reasonably practicable after receiving it? [§716.7(e)]</p> <p>30. Does the credit union allow the consumer to opt out at any time? [§716.7(f)]</p> <p>31. Does the credit union continue to honor the consumer's opt out direction until revoked by the consumer in writing, or, if the consumer agrees, electronically? [§716.7(g)(1)]</p>
<p><u>Yes</u></p>	<p><u>No</u></p>	<p>32. When a member relationship ends, does the credit union continue to apply the member's opt out direction to the nonpublic personal information collected during, or related to, that specific member relationship (but not to new relationships, if any, subsequently established by that member)? [§716.7(g)(2)]</p> <p>Revised Notices</p> <p>33. Except as permitted by §716.13-§716.15, does the credit union refrain from</p>

		<p>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:</p> <ul style="list-style-type: none"> a. the credit union has provided the consumer with a clear and conspicuous revised notice that accurately describes its privacy policies and practices; [§716.8(a)(1)] b. the credit union has provided the consumer with a new opt out notice; [§716.8(a)(2)] c. the credit union has given the consumer a reasonable opportunity to opt out of the disclosure, before disclosing any information; [§716.8(a)(3)] and d. the consumer has not opted out? [§716.8(a)(4)] <p>34. Does the credit union deliver a revised privacy notice when it:</p> <ul style="list-style-type: none"> a. discloses a new category of nonpublic personal information to a nonaffiliated third party; [§716.8(b)(1)(i)] b. discloses nonpublic personal information to a new category of a nonaffiliated third party; [§716.8(b)(1)(ii)] or c. discloses nonpublic personal information about a former member to a nonaffiliated third party, if that former member has not had the opportunity to exercise an opt out right regarding that disclosure? [§716.8(b)(1)(iii)] <p><i>(Note: A revised notice is not required if the credit union adequately described the nonaffiliated third party or information to be disclosed in the prior privacy notice. [§716.8(b)(2)])</i></p> <p>Delivery Methods</p> <p>35. Does the credit union 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? [§716.9(a)]</p> <p>36. Does the credit union use a reasonable means for delivering the notices, such as:</p> <ul style="list-style-type: none"> a. hand-delivery of a printed copy; [§716.9(b)(1)(i)] b. mailing a printed copy to the last known address of the consumer; [§716.9(b)(1)(ii)]
<p><u>Yes</u></p>	<p><u>No</u></p>	<ul style="list-style-type: none"> c. for the consumer who conducts transactions electronically, clearly and conspicuously posting the notice on the credit union’s electronic site and requiring the consumer to acknowledge receipt as a necessary step to obtaining a financial product or service; [§716.9(b)(1)(iii)] or 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? [§716.9(b)(1)(iv)] <p><i>(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 member who does not obtain products or</i></p>

services electronically. [§716.9 (b)(2)(i) and (ii), and (d)]

37. For annual notices only, if the credit union does not employ one of the methods described in question 36, does it employ one of the following reasonable means of delivering the notice such as:
 - a. for the member who uses the credit union’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; [§716.9(c)(1)] or
 - b. for the member who has requested the credit union refrain from sending any information about the member relationship, making copies of the current privacy notice available upon member request? [§716.9(c)(2)]

38. For members only, does the credit union ensure that the initial, annual, and revised notices may be retained or obtained later by the member in writing, or if the member agrees, electronically? [§716.9(e)(1)]

39. Does the credit union 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; [§716.9(e)(2)(i)]
 - b. mailing a printed copy to the last known address of the member; [§716.9(e)(2)(ii)] or
 - c. making the current privacy notice available on the credit union’s Web site (or via a link to the notice at another site) for the member who agrees to receive the notice at the Web site? [§716.9(e)(2)(iii)]

40. Does the credit union provide at least one initial, annual, and revised notice, as applicable, to joint consumers? [§716.9(g)]

<u>Yes</u>	<u>No</u>	
		<p>SUBPART B Limits on Disclosure to Nonaffiliated Third Parties</p> <p>41. Does the credit union refrain from disclosing any nonpublic personal information about a consumer to a nonaffiliated third party, other than as permitted under §716.13-§716.15, unless:</p> <ul style="list-style-type: none"> a. it has provided the consumer with an initial notice; [§716.10(a)(1)(i)] b. it has provided the consumer with an opt out notice; [§716.10(a)(1)(ii)] c. it has given the consumer a reasonable opportunity to opt out before the disclosure; [§716.10(a)(1)(iii)] and d. the consumer has not opted out? [§716.10(a)(1)(iv)] <p><i>(Note: This disclosure limitation applies to consumers as well as to members [§716.10(b)(1)], and to all nonpublic personal information regardless of whether collected before or after receiving an opt out direction. [§716.10(b)(2)])</i></p> <p>42. Does the credit union provide the consumer with a reasonable opportunity to opt out such as by:</p> <ul style="list-style-type: none"> a. mailing the notices required by §716.10 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; [§716.10(a)(3)(i)] b. where the consumer opens an on-line account with the credit union and agrees to receive the notices required by §716.10 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; [§716.10(a)(3)(ii)] or c. for isolated transactions, providing the notices required by §716.10 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? [§716.10(a)(3)(iii)] <p>43. Does the credit union allow the consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out? [§716.10(c)]</p> <p><i>(Note: A credit union may allow partial opt outs in addition to, but may not allow them instead of, a comprehensive opt out.)</i></p> <p>Limits on Redislosure and Reuse of Information</p> <p>44. If the credit union receives information from a nonaffiliated financial institution under an exception in §716.14 or §716.15, does the credit union refrain from using or disclosing the information except:</p>
		<ul style="list-style-type: none"> a. to disclose the information to the affiliates of the financial institution from which it received the information; [§716.11(a)(1)(i)]

<u>Yes</u>	<u>No</u>	
		<p>b. to disclose the information to its own affiliates, which are in turn limited by the same disclosure and use restrictions as the recipient credit union; [§716.11(a)(1)(ii)] and</p> <p>c. to disclose and use the information pursuant to an exception in §716.14 or §716.15 in the ordinary course of business to carry out the activity covered by the exception under which the information was received? [§716.11(a)(1)(iii)]</p> <p><i>(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, a credit union receiving information for fraud-prevention purposes could provide the information to its auditors. But “in the ordinary course of business” does not include marketing. [§716.11(a)(2)])</i></p> <p>45. If the credit union receives information from a nonaffiliated financial institution other than under an exception in §716.14 or §716.15, does the credit union refrain from disclosing the information except:</p> <p>a. to the affiliates of the financial institution from which it received the information; [§716.11(b)(1)(i)]</p> <p>b. to its own affiliates, which are in turn limited by the same disclosure restrictions as the recipient credit union; [§716.11(b)(1)(ii)] and</p> <p>c. to any other person, if the disclosure would be lawful if made directly to that person by the institution from which the recipient credit union received the information? [§716.11(b)(1)(iii)]</p> <p>Limits on Sharing Account Number Information for Marketing Purposes</p> <p>46. Does the credit union 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, share account, or transaction account to any nonaffiliated third party (other than to a consumer reporting agency) for telemarketing, direct mail or electronic mail marketing to the consumer, except:</p> <p>a. to the credit union's agents or service providers solely to market the credit union's own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account; [§716.12(b)(1)] or</p> <p>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 member when the member enters into the program? [§716.12(b)(2)]</p>
		<p><i>(Note: An “account number or similar form of access number or access code” does not include numbers in encrypted form, so long as the credit union does not provide the recipient with a means of decryption. [§716.12(c)(1)] A transaction account does not include an account to which third parties cannot initiate charges. [§716.12(c)(2)])</i></p>

<u>Yes</u>	<u>No</u>
	<p>SUBPART C Exception to Opt Out Requirements for Service Providers and Joint Marketing</p> <p>47. If the credit union discloses nonpublic personal information to a nonaffiliated third party without permitting the consumer to opt out, do the opt out requirements of §716.7 and §716.10, and the revised notice requirements in §716.8, not apply because:</p> <ul style="list-style-type: none"> a. the credit union disclosed the information to a nonaffiliated third party who performs services for or functions on behalf of the credit union (including joint marketing of financial products and services offered pursuant to a joint agreement as defined in paragraph (b) of §716.13); [§716.13(a)(1)] b. the credit union has provided consumers with the initial notice; [§716.13(a)(1)(i)] and c. the credit union 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 §716.14 or §716.15 in the ordinary course of business to carry out those purposes? [§716.13(a)(1)(ii)] <p>Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions</p> <p>48. If the credit union discloses nonpublic personal information to nonaffiliated third parties, do the requirements for initial notice in §716.4(a)(2), opt out in §716.7 and §716.10, revised notice in §716.8, and for service providers and joint marketing in §716.13, 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:</p> <ul style="list-style-type: none"> a. servicing or processing a financial product or service requested or authorized by the consumer; [§716.14(a)(1)] b. maintaining or servicing the consumer's account with the credit union or with another entity as part of a private label credit card program or other credit extension on behalf of the entity; or [§716.14(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? [§716.14(a)(3)] <p>49. If the credit union uses a §716.14 exception as necessary to effect, administer, or enforce a transaction, is it :</p> <ul style="list-style-type: none"> a. required, or is one of the lawful or appropriate methods to enforce the rights of the credit union or other persons engaged in carrying out the transaction or providing the product or service; [§716.14(b)(1)] or
<u>Yes</u>	<u>No</u>
	<ul style="list-style-type: none"> b. required, or is a usual, appropriate, or acceptable method to:[§716.14(b)(2)]

		<ul style="list-style-type: none"> 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; [§716.14(b)(2)(i)] ii. administer or service benefits or claims; [§716.14(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; [§716.14(b)(2)(iii)] iv. accrue or recognize incentives or bonuses; [§716.14(b)(2)(iv)] v. underwrite insurance or for reinsurance or for certain other purposes related to a consumer's insurance; [§716.14(b)(2)(v)] or vi. in connection with: <ul style="list-style-type: none"> (1) the authorization, settlement, 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; [§716.14(b)(2)(vi)(A)] (2) the transfer of receivables, accounts or interests therein; [§716.14(b)(2)(vi)(B)] or (3) the audit of debit, credit, or other payment information? [§716.14(b)(2)(vi)(C)] <p>Other Exceptions to Notice and Opt Out Requirements</p> <p>50. If the credit union discloses nonpublic personal information to nonaffiliated third parties, do the requirements for initial notice in §716.4(a)(2), opt out in §716.7 and §716.10, revised notice in §716.8, and for service providers and joint marketers in §716.13, not apply because the credit union makes the disclosure:</p> <ul style="list-style-type: none"> a. with the consent or at the direction of the consumer; [§716.15(a)(1)] <ul style="list-style-type: none"> i. to protect the confidentiality or security of records; [§716.15(a)(2)(i)] ii. to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; [§716.15(a)(2)(ii)] iii. for required institutional risk control or for resolving consumer disputes or inquiries; [§716.15(a)(2)(iii)] iv. to persons holding a legal or beneficial interest relating to the consumer; [§716.15(a)(2)(iv)] or v. to persons acting in a fiduciary or representative capacity on behalf of the consumer; [§716.15(a)(2)(v)]
<u>Yes</u>	<u>No</u>	<ul style="list-style-type: none"> b. to insurance rate advisory organizations, guaranty funds or agencies, agencies rating the credit union, persons assessing compliance, and the credit union's attorneys, accountants, and auditors; [§716.15(a)(3)] c. in compliance with the Right to Financial Privacy Act, or to law enforcement agencies; [§716.15(a)(4)]

- d. to a consumer reporting agency in accordance with the FCRA or from a consumer report reported by a consumer reporting agency; [§716.15(a)(5)]
- e. 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; [§716.15(a)(6)]
- f. to comply with Federal, state, or local laws, rules, or legal requirements; [§716.15(a)(7)(i)]
- g. to comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities; [§716.15(a)(7)(ii)] or
- h. to respond to judicial process or government regulatory authorities having jurisdiction over the credit union for examination, compliance, or other purposes as authorized by law? [§716.15(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 [a credit union’s] disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to [the credit union] for a mortgage so that the insurance company can offer homeowner’s insurance to the consumer.”)