National Credit Union Administration

Privacy of Consumer Financial Information:

Small Credit Union Compliance Guide

Table of Contents

Introduction

Title V of the Gramm-Leach-Bliley Act ("GLBA" or "the Act") requires a financial institution to notify all of its customers about its privacy policies and practices with respect to disclosing information to its affiliates and nonaffiliated third parties. The Act prohibits a financial institution, subject to certain exceptions, from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution satisfies various notice requirements and the consumer has not elected to opt out of the disclosure.

The National Credit Union Administration (NCUA) issued regulations implementing the privacy provisions of the Act. 12 C.F.R. Part 716. NCUA's regulations are referred to as "the consumer privacy rule" throughout this compliance guide. This guide includes references to sections in the regulation, for example, "§716.13," so users can refer to the regulation.

NCUA's consumer privacy rule was developed in coordination with the other regulators of financial institutions: the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), the Office of Thrift Supervision ("OTS"), and the Board of Governors of the Federal Reserve System ("FRB"); the Federal Trade Commission ("FTC"), and the Securities and Exchange Commission ("SEC") (collectively, the "Agencies"). Each of the other Agencies has also issued regulations to implement the privacy provisions of GLBA, which are comparable and consistent with NCUA's consumer privacy rule. The Agencies consulted with representatives of state insurance authorities in the process of issuing their regulations. The Commodity Futures Trading Commission ("CFTC") recently also issued comparable and consistent regulations.

Although the consumer privacy rule had an effective date of November 13, 2000, mandatory compliance was delayed until July 1, 2001, to provide sufficient time for credit unions to develop the necessary notices and procedures to be in full compliance with the rule. Section I.F. of this guide describes the requirements that apply to a credit union on the compliance date.

NCUA has addressed this small credit union compliance guide to all federally-insured credit unions. NCUA refers to them as "a credit union" or "you" throughout this compliance guide. NCUA has issued this small credit union compliance guide in accordance with the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857, reprinted in 5 U.S.C. 601, note (West 1996). This small credit union compliance guide supplements the NCUA's regulations but is not a substitute for any provision of the regulations.

I. Summary of Key Provisions of the Consumer Privacy Rule

A. General Principles of the Consumer Privacy Rule

The consumer privacy rule embodies two general principles — notice and opt out.

- A credit union must provide clear and conspicuous privacy notices to its consumers that accurately describe the credit union's information policies and practices regarding the treatment of nonpublic personal information. A credit union must give members an initial privacy notice not later than the time of establishing the member relationship and annually during the continuation of the member relationship. A credit union must give consumers who are not members an initial privacy notice only if the credit union intends to disclose nonpublic personal information about them with nonaffiliated third parties other than under the exceptions for servicing or processing transactions (see §§ 716.14, 716.15). A credit union has no obligations under the consumer privacy rule with respect to a member business or nonmember conducting business transactions.

- A credit union must provide each consumer with a reasonable opportunity to prevent, or opt out of, the disclosure of nonpublic personal information to nonaffiliated third parties. The consumer privacy rule contains a number of exceptions to this general requirement to allow disclosures to process transactions, service a consumer's account, and facilitate other normal business transactions (see §§ 716.13, 716.14, and 716.15).

If a credit union intends to disclose nonpublic personal information outside of the exceptions, it must provide consumers with an opt out notice and a reasonable means and time to exercise the opt out before disclosing nonpublic personal information to nonaffiliated third parties. The credit union may combine the opt out notice with the initial notice, but cannot issue the opt out notice by itself.

If a credit union is disclosing nonpublic personal information outside the exceptions, it must provide each of its consumers with an initial privacy policy notice, an opt out notice, and a reasonable opportunity to exercise the opt out right. Since July 1, 2001, credit unions have been prohibited from disclosing the information about a consumer until they provide the notices and reasonable opportunity to opt out.

B. Key Terms

To understand the scope and application of the consumer privacy rule, it is important to understand key terms used throughout the rule, in particular:

- Nonpublic personal information, personally identifiable financial information, and publicly available information;
- Consumers, customers, and members; and
- Nonaffiliated third party.

1. Nonpublic Personal Information, Personally Identifiable Financial Information, and Publicly Available Information (§716.3(q)-(s))

The rule identifies three primary categories of information: nonpublic personal information, personally identifiable financial information, and publicly available information.

Nonpublic personal information is the category of information protected by the consumer privacy rule. The definitions for personally identifiable financial information and publicly available information work together to describe and define nonpublic personal information. Each term is described in more detail below.

- Personally identifiable financial information is any information that a credit union collects about a consumer in connection with providing a financial product or service. This includes:

    - information provided by the consumer during the application process (e.g., name, phone number, address, income);
    - information resulting from the financial product or service transaction (e.g., payment history, loan or deposit balances, credit card purchases); or
    - information from other sources about the consumer obtained in connection with providing the financial product or service (e.g., information from a consumer credit report or from court records).

Personally identifiable financial information also includes any information that "is disclosed in a manner that indicates that the individual is or has been your consumer" (see §716.3(r)(3)(i)(D)). The fact that an individual is a consumer of a credit union is personally identifiable financial information about that consumer.

- Publicly available information is any information that a credit union has a reasonable basis to believe is lawfully publicly available. Because a "reasonable basis to believe" is an important part of the definition of publicly available information, the consumer privacy rule specifically defines this phrase. The definition states that a reasonable basis exists where a credit union has taken steps to determine (a) that the information is of the type that is generally available to the public and (b) whether the individual has blocked the information from being made available to the general public if they have the ability to do so. This means that a credit union should consider a member's phone number to be publicly available only if the credit union takes steps to determine that the phone number is listed. Similarly, a credit union may consider all mortgage documents and assessed values to be publicly available if state and local laws require all that information to be filed in the public record.

- Nonpublic personal information, the category of information protected by the consumer privacy rule, consists of:
  (1) personally identifiable financial information that is not publicly available information; and

(2) lists, descriptions, or other groupings of consumers, which may contain publicly available information about them, but either contain or are created using personally identifiable financial information that is not publicly available information.

The first category of nonpublic personal information consists of personally identifiable financial information that is not publicly available information.

The second category of information protected by the rule consists of certain "lists, descriptions, or other groupings." A list is considered nonpublic personal information if it is created based on member relationships, loan balances, account numbers, or other personally identifiable financial information that is not publicly available. If credit union has generated a list or other grouping of consumers by using personally identifiable financial information, then all of the information contained in that list — including the publicly available information about those consumers — is covered as nonpublic personal information.

Lists or other groupings that are created using only publicly available information and that contain only publicly available information are excluded from the definition of nonpublic personal information. For example, in a jurisdiction where mortgage documents are public records, a list of the names and addresses contained in those records of individuals for whom a credit union held a mortgage would be outside the definition of nonpublic personal information if the credit union creates that list using publicly available information. The list would become nonpublic personal information, however, if it contains current loan balances or if it was created using other personally identifiable financial information, such as current mortgage loan balances in excess of a certain amount.

2. Consumers, Customers, and Members (§716.3(e), (i), and (n))

A consumer is an individual 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 consumer may be a member or nonmember of the credit union. A consumer includes an individual's legal representative. A consumer also includes someone involved in an isolated transaction, such as using an ATM at a credit union where the person does not have a member relationship.

A "financial product or service" (§716.3(m)) includes, among other things, a credit union's evaluation 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 a credit union's evaluation of a membership application. Based on the definition of "financial product or service," an individual who applies for membership is a consumer regardless of whether the individual actually joins the credit union.

A customer is a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship between a consumer

and a financial institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

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

For example, a consumer establishes a member relationship with a credit union when he or she:

- becomes a member of the credit union as defined in its bylaws;
- is a nonmember and opens a credit card account jointly with a member under the credit union's procedures;
- is a nonmember and executes a contract to open a share or share draft with the credit union or obtains credit from the credit union jointly with a member, including an individual acting as a guarantor;
- is a nonmember and opens an account with a credit union that has been designated as a low-income credit union; or
- is a nonmember and opens an account under state law with a state-chartered credit union.

The consumer privacy rule recognizes that certain member relationships terminate. A credit union is not required to provide its annual privacy notice to a former member or a nonmember who has a member relationship with the credit union whose account is inactive. But, a credit union must continue to comply with an opt out instruction of a former member.

3. Nonaffiliated Third Parties (§716.3(p))

The consumer privacy rule restricts the disclosure of nonpublic personal information to nonaffiliated third parties. A nonaffiliated third party is any person except a credit union's affiliate or a person employed jointly by the credit union and a company that is not the credit union's affiliate. An "affiliate" (§ 716.3(a)) of a credit union is any company that controls, is controlled by, or is under common control with the credit union. Affiliates include a federal credit union's credit union service organizations (CUSOs) and any company that a state-chartered credit union controls. NCUA will presume a credit union controls a CUSO if it is 67% owned by one or more credit unions.

C. Prohibition against the Disclosure of Account Numbers (§716.12)

A credit union must not disclose an account number or similar form of access number or access code to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. This prohibition against disclosing account numbers for marketing purposes applies even

under a joint agreement to market financial products or services permitted under §716.13. The disclosure of an encrypted account number, however, is not prohibited as long as the credit union does not disclose the key to decrypt the number.

There are three exceptions to this prohibition: (1) to a consumer reporting agency, as stated in the general provision in §716.12(a); (2) to an agent or service provider to market a credit union's own products or services, as long as the agent or service provider is not authorized to initiate charges directly to the account; or (2) to participants in a private label or affinity credit card program, as long as those participants are identified to the member when he or she enters the program.

D. Limitations on the Redisclosure and Reuse of Information (§716.11)

A credit union that receives nonpublic personal information from a nonaffiliated financial institution is limited in its ability to use or disclose that information later. The precise limits on reuse or redisclosure depend on the reason the credit union received the information.

- If the credit union receives information under one of the exceptions for servicing or processing a transaction (§§ 716.14 or 716.15), the credit union may disclose and use that information as permitted under both of those exceptions. For example, a credit union that receives information to process a transaction may also disclose that information in response to an authorized subpoena or to its auditors, so that the credit union may continue to conduct routine business. The credit union may not reuse or redisclose the information for marketing purposes.

- If a credit union receives information from a nonaffiliated financial institution other than under one of the exceptions for servicing or processing a transaction or other general exceptions (§§ 716.14 or 716.15), then the credit union "steps into the shoes" of the financial institution that provided the information. The credit union may use the information for its own purposes, including marketing, and may disclose that information to other nonaffiliated third parties in a manner that is consistent with the privacy policy of the financial institution that provided the information. For example, a credit union that receives another financial institution's consumer list could redisclose that list to other non-financial companies if that disclosure would be consistent with the opt out and privacy notices provided by the financial institution to the consumers about whom the information relates. The credit union also may disclose that information, for example, in response to an authorized subpoena or to its auditors.

- The credit union must follow the consumer's opt out election for any consumer information it possesses. Thus, the credit union would have to keep track of any opt out decisions by the consumers if the credit union intends to disclose information except as permitted to service or process transactions (§§ 716.14 or 716.15).

- Regardless of the purposes for which a credit union has obtained information, it may disclose it to the affiliates of the financial institution from which it received the information.

- A recipient of information may disclose it to its own affiliates. The affiliate may, in turn, disclose and use the information only to the extent permissible for its affiliate from which it received the information.

E. Relation to Other Laws

1. Fair Credit Reporting Act (FCRA)

The consumer privacy rule does not limit or supersede the operation of the FCRA.

2. State Laws

The consumer privacy rule does not affect any state statute, regulation, order, or interpretation that is more protective of the consumer than the regulation. GLBA authorizes the FTC to make the determination after consulting with the Agencies.

F. Effective Date

Compliance with the consumer privacy rule became mandatory on July 1, 2001, requiring a credit union to provide an initial privacy notice to members not later than July 1, 2001. A credit union that disclosed its consumers' nonpublic personal information to a nonaffiliated third party, other than under the exceptions for processing and servicing transactions and other general exceptions, and wishes to continue the disclosures after July 1, 2001, must provide the consumers with privacy and opt out notices and reasonable opportunity to opt out before continuing to disclose the information. As of July 1, 2001, a credit union must provide its initial privacy notice to new members even if the credit union does not disclose nonpublic personal information with any nonaffiliated third parties.

II. Basic Requirements of the Consumer Privacy Rule and Disclosures Under the Exceptions

This section describes the basic requirements of the consumer privacy rule, such as how and when to deliver the privacy notices. This section also describes the obligations if a credit union only discloses nonpublic personal information as permitted under the exceptions.

A credit union that does not have any affiliates and discloses nonpublic personal information to nonaffiliated third parties only under the exceptions (§§ 716.13, 716.14,

and 716.15) faces relatively fewer compliance burdens under the consumer privacy rule. In general, if a credit union only discloses nonpublic personal information to nonaffiliated third parties as permitted under the exceptions to process or service transactions or other general exceptions (§§ 716.14 and 716.15), then the credit union only needs to provide initial and annual notices to its members. It does not need to provide opt out notices or revised privacy notices to its members; to provide any notices to its consumers who are not members, such as an individual who uses the credit union's ATM but does not maintain any member relationship with that credit union.

A credit union may disclose or reserve the right to disclose, nonpublic personal information, such as its member lists, as part of marketing arrangements with other financial institutions, such as an insurance company or broker-dealer, subject to certain conditions. While these types of disclosures are not within the scope of the exceptions to process or service transactions or other general exceptions (§§716.14 or 716.15), the parties may design their marketing arrangements to qualify as joint agreements under §716 .13.

A. Basic Requirements of the Consumer Privacy Rule

1. Delivery of Privacy Notices

In general, a credit union must deliver notices so that the consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically (§716.9(a)). For example, the initial notice may be mailed or hand-delivered to a consumer with a membership agreement. For a consumer who applies for membership through the credit union's web site, the credit union may post the notice on the site and require the consumer to agree to receive the notice through the web site as a necessary step to becoming a member (§716.9(e)). In addition, for members only, a credit union must provide the initial, annual, and revised notices so that the member can retain or obtain them later in writing or, if the member agrees, electronically.

A credit union must provide an initial privacy notice to each of its members, even if the credit union shares nonpublic personal information with nonaffiliated third parties only under the exceptions. For instance, a credit union must provide an initial notice to an individual who becomes a member. By contrast, a consumer who uses Credit Union A's ATM to withdraw funds from a checking account at Bank B is not Credit Union A's member as a result of that transaction, even though the individual is a consumer of Credit Union A. Even if the individual repeatedly uses Credit Union A's ATM, that individual is not Credit Union A's member.

2. Time to Provide Initial Notice

A credit union must provide notice to members of its privacy policies and practices at various times.

- A credit union must provide an initial notice that accurately describes its privacy policies and practices to a new member not later than when the credit union establishes a member relationship (§ 716.4(a)(1)). For instance, a privacy notice must be provided to an individual not later than when that individual signs the membership agreement. Thus, a credit union can provide the notice to a new member together with the membership agreement and signature card. A credit union may always deliver a privacy notice earlier than required.

- Subsequent delivery of the initial notice is allowed only under two circumstances: (1) if establishing the member relationship is not at the consumer's election; or (2) if providing the notice at the time of the election would substantially delay the member's transaction and the member agrees to receive the notice at a later time.

- If an existing member obtains a new financial product or service, then the credit union is not required to provide another initial notice to that member (§716.4(d)) if the earlier notice covers the product. For instance, if Joe Smith becomes a member of XYZ Credit Union, it complies with §716.4(a)(1) if it provides an initial notice to Joe together with the membership agreement. Joe becomes a member of XYZ Credit Union when he signs the membership agreement. If Joe remains a member and, six months later, applies to XYZ Credit Union for a loan, XYZ Credit Union is not required to provide another initial notice to Joe if the initial notice that Joe received when he became a member is accurate with respect to his loan account.

- If a credit union discloses information about a consumer, even a consumer who is not a member, outside of the exceptions described in this section, then before making that disclosure, it must provide an initial notice, an opt out notice, and a reasonable opportunity for the consumer to opt out of that disclosure. See section III below.

3. Annual Notice

During the continuation of the member relationship, a credit union must provide an annual notice to the member, as described in §716.5(a). A credit union is not required to provide an annual notice to an individual who no longer has a member relationship with the credit union. Thus, for instance, if Sally Smith terminates her membership with ABC Credit Union, it would have no further obligation to provide Sally an annual notice. If Sally terminates her membership at ABC Credit Union, and later rejoins, Sally would be entitled to a new initial privacy notice when she rejoins and annual notices while she is a member.

4. Method of Providing the Annual Notice

Like the initial notice, the annual notice must be delivered so that each member can reasonably be expected to receive actual notice, in writing or, if the member agrees, electronically (§ 716.9(a)). A credit union may satisfy this requirement by mailing a printed copy of the notice to the member's last known address. For members who use the credit union's web site to access financial products and services, such as electronic bill payment, and who agree to receive notices at the web site, a credit union may reasonably expect these members to receive actual notice by continuously posting its current privacy notice on the web site in a clear and conspicuous manner.

5. Joint Accounts

A credit union may provide a single initial notice to two or more members who jointly obtain a financial product or service, other than a loan. The credit union is required to provide an initial notice to a borrower or guarantor on a loan, who is not otherwise a member, if the credit union shares his or her nonpublic personal information with nonaffiliated third parties as permitted by the rule's exceptions (§716.4(d)(6)(i)). The credit union may satisfy the annual notice requirement by providing one notice to joint members and borrowers and guarantors (§§ 716.9(g), 716.7(d)(6)(ii)).

6. Information Described in the Initial and Annual Notices

Credit unions that only disclose nonpublic personal information to nonaffiliated third parties under the exceptions to process or service transactions or other general exceptions (§§ 716.14 and 716.15), may provide simplified initial and annual notices. These simplified notices must include a description of the following items of information:

- the categories of nonpublic personal information that the credit union collects (§ 716.6(a)(1));
- that the credit union does not disclose nonpublic personal information about current and former members to affiliates or nonaffiliated third parties, except to service or process transactions (§716.6(a)(2)-(4)). When describing the categories of the parties, the notice may state that the credit union makes disclosures to the other parties as permitted by law (§716.6(b)); and
- the credit union's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (§716.6(a)(8)).

For each of these information items above, a credit union may use a sample clause from Appendix A of Part 716. NCUA emphasizes that a sample clause may be used only if that clause accurately describes the credit union's actual policies and practices. The following are examples of required elements of the privacy notice for those credit unions*:*

- *XYZ Credit Union collects nonpublic personal information about you from the following sources:*

(1) information we receive from you on applications or other forms;

(2) information about your transactions with us or others; and

(3) information we receive from a consumer reporting agency.

- *We do not disclose any nonpublic personal information about you to anyone, except as permitted by law.*

- *If you decide to close your account(s) or become an inactive member, we will adhere to the privacy policies and practices as described in this notice.*

- *XYZ Credit Union restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. XYZ Credit Union maintains physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.*

7. Additional Elements in the Privacy Notice for Credit Unions that Disclose Information by Agreements with Service Providers and Joint Marketers (§ 716.13).

If a credit union discloses nonpublic personal information in accordance with the exception for agreements with service providers that do not fall within the exceptions to service or process transactions and joint marketers, the credit union's privacy notice must include an accurate description of those arrangements. The privacy notice must describe the categories of information the credit union discloses under these arrangements and the categories of third parties with whom the credit union has contracted. The following sample clause, if applicable, is sufficient to comply with the requirements of §716.6(a)(5):

We may disclose all of the information we collect, as described [describe location in the notice, such as "*above*" or "*below*"] *to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.*

8. Initial and Annual Notices Must Be Clear and Conspicuous

NCUA emphasizes that the initial and annual notices must be clear and conspicuous, as defined in §716.3(b). Clear and conspicuous means that a notice is

both (1) reasonably understandable and (2) designed to call attention to the nature and significance of the information in the notice. This general standard applies to various media and the consumer privacy rule provides several examples of ways in which a credit union can present its notice in a manner that complies with the rule.

B. Exceptions for Processing and Servicing Transactions and other General Exceptions

A credit union may disclose nonpublic personal information to nonaffiliated third parties under the exceptions process or service transactions or other general exceptions (§§ 716.14 and 716.15) without triggering the notice and opt out requirements for consumers. While the credit union must provide its members with initial and annual privacy notices, the notices may refer to the categories of nonaffiliated third parties to whom it discloses the information under these exceptions as "permitted by law" (see §716.6(b)). The exceptions in §716.14 generally permit credit unions to disclose member information freely to carry out routine business transactions involving existing accounts. For example, a credit union may disclose nonpublic personal information to a nonaffiliated third party to:

(1) service the credit union's mortgages,
(2) securitize its loans or sell them on the secondary market,
(3) prepare or mail account statements,
(4) make account information available to the credit union's members on its web site,
(5) verify the sufficiency of funds in an account to cover a member's check,
(6) collect a share draft, or
(7) collect a debt.

Section 716.15 provides additional general exceptions to the notice and opt out requirements that permit credit unions to disclose member information to nonaffiliated third parties. A credit union may disclose nonpublic personal information where a consumer has consented and does not revoke the consent to the specific disclosure, for example, where a member has applied for a mortgage and consents to the credit union's sharing that fact with a nonaffiliated insurance company so the insurance company can offer the member homeowner's insurance. A credit union may also disclose nonpublic personal information under this exception to comply with a properly authorized subpoena or with federal, state, or local laws. Other permissible arrangements under §716.15 include disclosures of information to:

(1) a nonaffiliated third party software vendor to protect the confidentiality or security of the credit union's member records,
(2) a person acting in a fiduciary or representative capacity on behalf of the consumer,
(3) the credit union's auditors, attorneys, and accountants,
(4) a consumer reporting agency in accordance with the Fair Credit Reporting Act, or

(5) a law enforcement agency in accordance with the Right to Financial Privacy Act.

C. Exception for Agreements with Services Providers and Joint Marketers (§716.13)

Section 716.13 permits a credit union to disclose nonpublic personal to nonaffiliated third parties that perform services or functions for the credit union without providing opt out notices. To do this, a credit union must satisfy two conditions. First, the credit union must describe the disclosure in its privacy notices to its members. Second, the credit union must have an agreement with the recipient that prohibits it from using the information other than for the purposes for which it received the information (see §716.13(a)(1)(ii)).

For example, under this exception, a credit union may arrange with a nonaffiliated third party, such as a telemarketer or direct mail marketer, to market the credit union's own products or services. Also, a credit union may provide nonpublic personal information to another financial institution as part of a "joint agreement." Under the joint agreement, the credit union and the financial institution would agree in writing to jointly offer, sponsor, or endorse certain financial products or services. (see §716.13(c)). The consumer privacy rule does not impose any particular requirements regarding the form, scope, duration, or other terms of the parties' agreement.

The following arrangements are examples of joint agreements:

- An agreement under which a credit union provides its member list to a broker-dealer to solicit the credit union's members for investment services, and the broker-dealer pays the credit union for any referrals. Under this agreement, the credit union and broker-dealer must jointly offer, sponsor, or endorse the investment services the broker-dealer is providing to the members.

- An agreement under which a credit union provides a list of its electronic banking members to a financial information aggregation service provider to solicit the credit union's members for Internet transaction services and is compensated by any referrals. Under this agreement, the credit union and the aggregator must jointly offer, sponsor, or endorse the Internet transaction services the aggregator is providing to the members.

III. Disclosures Outside of the Exceptions

This section addresses additional requirements that apply to credit unions that disclose nonpublic personal information to affiliates or to nonaffiliated third parties

outside of the enumerated exceptions. Those credit unions must describe the disclosures in their initial and annual notices, as well as give a reasonable opportunity for consumers to opt out of those disclosures.

A. Describing the Disclosures in the Initial and Annual Privacy Notices

The consumer privacy rule requires a credit union that discloses nonpublic personal information outside of the exceptions to include in its notices the following additional items:

1. The categories of nonpublic personal information that a credit union discloses. A credit union may satisfy this requirement by listing the sources of the information (e.g., from the consumer, from transactions with the consumer, or from consumer reporting agencies) and providing a few examples to illustrate the types of information in each category.

2. The categories of third parties, both affiliates and nonaffiliated third parties, to whom the credit union discloses nonpublic personal information not covered by an exception. A credit union may satisfy this requirement by stating that it discloses to financial service providers, non-financial companies, and others (as applicable) and providing a few examples to illustrate the types of entities in each category.

3. If the credit union discloses nonpublic personal information about former members to third parties, a description of the categories of the information and the third parties.

4. Any notice that the credit union provides under the FCRA concerning the ability of a consumer to opt out of disclosures of information to affiliates.

Because the requirements to describe each of these items for the initial and annual notices are identical, a credit union may use the same form for both notices, if that form is accurate.

A credit union also may elect to provide a short-form notice to consumers who do not become members of the credit union (§ 716.6(d)). This situation could arise, for instance, when a consumer uses the credit union's ATM, but is not a member. Generally, if the credit union wants to disclose information about the consumer to third parties other than under the exceptions, then it must provide its privacy notice and opt out notice. A credit union may satisfy the privacy notice requirement by informing the consumer that a copy of the full privacy notice is available upon request and explaining

how he or she may obtain that notice. As with all notices required under the consumer privacy rule, the short-form notice must be: in writing, or, if the consumer agrees, in electronic form; clear and conspicuous; and accurate. This short-form notice must be accompanied by an opt out notice, as described below.

B. Describing the Consumer's Right to Opt Out of Disclosures in the Opt Out Notice

Before disclosing any nonpublic personal information to a nonaffiliated third party about a consumer other than under an exception, a credit union must first inform the consumer:

1. that the credit union discloses, or reserves the right to disclose, the information;
2. that the consumer has the right to opt out of that disclosure; and
3. how the consumer may exercise the opt-out right.

A credit union will be deemed to have provided an adequate notice of items 1 and 2, above, if it identifies the categories of (a) nonpublic personal information that may be disclosed and (b) nonaffiliated third parties to whom the information is disclosed, and states that the consumer may opt out of the disclosures.

C. Providing a Reasonable Opportunity to Opt Out

A credit union must provide consumers with a reasonable opportunity to opt out before disclosing the information (§ 716.10(a)(1)(iii)). A reasonable opportunity to opt out depends upon the particular circumstances of the transaction and includes several factors, such as the means by which the credit union provides the initial notice, the method(s) a consumer may use to opt out, and the length of time the credit union waits after sending a notice before determining that the consumer has not opted out.

The consumer privacy rule provides three examples:

1. If the credit union provides the notice by mail, it provides a reasonable opportunity to opt out by allowing the consumer to opt out by mailing a form or calling a toll free number, or providing other reasonable means within 30 days from when the credit union mailed the notices.

2. If a member opens an account and agrees to receive the notices electronically, the credit union provides a reasonable means to opt out by allowing the member to opt out within 30 days after the date the member acknowledges receipt of the notices in conjunction with opening the account.

3. For an isolated transaction, such as the consumer's purchase of a traveler's check, the credit union provides the consumer with a reasonable opportunity to opt out if it provides the notices at the time of the transaction and requests that the consumer decide whether to opt out before completing the transaction.

A credit union may specify a particular method for opting out, provided that the method is reasonable for that consumer. A credit union cannot require consumers to prepare their own letters and send them in before honoring an opt out.

D. Providing an Opt Out Notice for Joint Accounts (§§ 716.4 and 716.7)

Other than for loans, a credit union only has to deliver the initial opt out notice to one party of a joint account. Any of the joint account holders, however, can exercise the right to opt out. The opt out notice provided to joint account holders must explain how the credit union will treat an opt out direction by a joint account holder and must give one joint account holder the ability to opt out on behalf of all joint account holders.

A credit union is required to provide an initial opt out notice to a borrower or guarantor on a loan if it shares his or her nonpublic personal information with nonaffiliated third parties other than for purposes under the exceptions (§§716.13, 716.14, and 716.15).

E. Revising Your Privacy Notices

When a credit union changes its privacy policies and practices, it may need to provide revised notices. If a credit union changes its policies and practices regarding disclosures to nonaffiliated third parties so that its most recent notices are inaccurate, then the credit union may not disclose the information unless it provides revised privacy and opt out notices.

For example, if a credit union's prior notices stated that it discloses only information obtained from the consumer (see §716. 6(c)(1)(i)) and the credit union later plans to disclose a different category of information, such as information about the consumer's transactions with it (see §716. 6(c)(1)(ii)), then the credit union may not share information until it provides revised notices and another opportunity to opt out to the consumer. A notice may remain accurate if the credit union intends to disclose the same categories of information to another company that fits within one of the categories of nonaffiliated third parties that it described in the previous notices.

F. Complying with a Consumer's Decision to Opt Out

A credit union that is disclosing nonpublic personal information and receives a consumer's instruction to opt out must stop disclosing that information as soon as reasonably practicable (§ 716. 7(e)). A consumer may exercise his or her right to opt

out at any time (§ 716. 7(f)). A consumer's direction to opt out is effective until he or she revokes it in writing, or if he or she agrees, electronically (§ 716. 7(g))

IV. General Measures to Develop Privacy Notices

The following measures may assist you in developing your initial and annual notices regarding your privacy policy and practices, as well as the opt out notice, if applicable.

A. Understanding How the Consumer Privacy Rule Affects Your Business

The consumer privacy rule affects several important aspects of a credit union's business operations. You should obtain full information from all relevant sources within your credit union about the ways in which you obtain, store, and disclose information about consumers. Although the consumer privacy rule does not affect how you use or disclose aggregate information about your consumers, you should consider whether any aggregate information about your consumers might, in fact, identify any particular consumer(s) in a list, description, or other grouping. The results of your review should assist you in determining the elements of your privacy policy and in writing your notices.

You should carefully review each of your business units with respect to three core elements of its operations.

1. Your Consumers

- Who are your consumers?
- Which consumers are your members?

2. Information about Your Consumers that You Collect

- What kinds of personally identifiable financial information about your consumers do you obtain; that is, what information about your consumers do you obtain in connection with providing a financial product or service?
- What kinds of personally identifiable financial information about your consumers do you organize or can you retrieve?
- What kinds of personally identifiable financial information about your consumers is publicly available information?
- What lists, descriptions, or other groupings of your consumers do you maintain?
- Which lists, descriptions, or other groupings of your consumers contain only publicly available information and are derived using only publicly available information?

3. Information about Your Consumers that You Disclose to Your Affiliates and Nonaffiliated Third Parties

- Which transactions that you perform for consumers involve using and disclosing their nonpublic personal information?
- To what extent do you use and disclose consumers' nonpublic personal information to provide financial products or services to them?
- To what extent do you use and disclose consumers' nonpublic personal information to maintain or service their accounts?
- Which services or functions performed on your behalf by third parties involve disclosing consumers' nonpublic personal information?
- Which agreements between you and one or more financial institutions to market financial products or services involve disclosing consumers' nonpublic personal information?
- Do you disclose consumers' nonpublic personal information to nonaffiliated third parties other than as permitted by an exception? If so, which types of nonaffiliated third parties receive consumers' nonpublic personal information from you?

B. Designing Your Privacy Notices

1. Create Categories of Information

The consumer privacy rule requires you to describe, among other things, the categories of nonpublic personal information that you collect and disclose. Conducting an inventory of all types of nonpublic personal information about your consumers that you can organize or retrieve, as suggested in the previous section, will help you to describe each of those categories accurately. From that inventory, you can determine which types of information — and under which circumstances — you disclose to affiliates and nonaffiliated third parties. In addition, you must consider whether the categories of information that you collect and disclose about your former members are different from your current members.

To reduce your future costs of designing revised notices, you should consider whether you want to reserve the right to collect and disclose other categories of consumers' nonpublic personal information. Anticipating which categories of nonpublic personal information you may later disclose to nonaffiliated third parties, other than as authorized by an exception, is a key aspect of coordinating your initial and annual privacy notices with your opt out notices.

2. Describe the Consumer's Right to Opt Out of Disclosures

If you disclose nonpublic personal information to nonaffiliated third parties, other than as permitted by an exception, you may need to conduct an inventory of all types of nonaffiliated third parties to whom you disclose nonpublic personal information so that you can accurately describe them in your notices. Similarly, you should consider whether the categories of nonpublic personal information that you collect are different from the categories you disclose. Accurately categorizing each of the types of nonpublic personal information and nonaffiliated third parties to whom you disclose is

particularly important if you provide choices to consumers concerning the scope of their opt out rights.

Your initial and annual notices must explain the consumer's right to opt out. That explanation consists of three basic elements:

- a description of the categories of nonpublic personal information and the nonaffiliated third parties to whom you disclose;
- a statement that the consumer has the right to opt out of that disclosure; and
- an explanation of how the consumer may communicate his or her decision to opt out.

3. Describe the Consumer's Right to Opt Out of Disclosures to Your Affiliates

If you disclose information about the consumer to your affiliates that triggers obligations under the FCRA, such as information from a credit report, then you must include an explanation of the consumer's right to opt out of that disclosure.

4. Describe Your Security Policies and Practices

Your privacy notice must include a description of your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. See NCUA's Guidelines Establishing Standards for Safeguarding Member Information, Appendix A to 12 C.F.R. Part 748.

5. Make Your Notices Clear and Conspicuous

Each of the elements of the consumers' right to opt out must be stated in terms that are reasonably understandable and presented in a manner that calls attention to the nature and significance of that information.

C. Delivering Your Initial and Annual Privacy Notices to Members

You must determine both how and when to deliver the initial and annual privacy notices to your members. Additionally, you should consider the special provisions for electronic delivery of notices.

1. Timing

You should consider identifying each of the methods by which your consumers become "members." For example, an individual may establish a member relationship with you during a visit to your branch office, while speaking to your representative over the telephone, or when signing up for membership through your web site. For each of these methods, you should identify when you can deliver the initial notice so that the individual can reasonably be expected to receive actual notice of your policy and practices not later than when the individual becomes a member.

2. Mechanisms for Delivering Notices

To ensure that you reliably deliver the notices so that each consumer can reasonably be expected to receive actual notice in writing, you should design systems that target delivery to an individual consumer. For instance, if a product involves sending an application to an individual's home address, you should consider including your initial notice with the application materials.

The systems you develop for delivering your notices may depend on whether you disclose (or reserve the right to disclose) consumers' nonpublic personal information to nonaffiliated third parties. If you plan to deliver a notice electronically, then you must design a system that reliably obtains the consumer's agreement to receive that notice electronically.

D. Providing a Reasonable Opportunity for Consumers to Opt Out of Disclosures

The systems and controls you use for delivering the opt out notices also must account for both the timing and the mechanism(s) of delivery. You must ensure that you have adequate systems and controls in place to receive and keep track of consumers' decisions to opt out. These systems may differ depending on the circumstances of the transaction or whether a member relationship exists.

The systems and controls you use to receive and keep track of consumers' decisions should themselves protect against unauthorized disclosure of their nonpublic personal information. You may, for example, establish a toll free telephone number that enables a consumer to enter an account number and communicate the decision to opt out of any disclosure relating to that account. Any system you use must include appropriate measures designed to accommodate any consumers' decisions to opt out at a later time or to revoke an opt out.

1. Member Transactions

If you mail the initial notice together with the opt out notice to the member's last known address, for example, then you should have a system that monitors the date the notices were sent so you can ensure you have provided the member an adequate time to respond to the notices.

2. Consumer Transactions

If you disclose, or reserve the right to disclose, a consumer's nonpublic personal information relating to a transaction in which there is no member relationship, you should consider how best to provide an opportunity for the consumer to opt out in light of the circumstances of that transaction. Because later communication with a consumer who is not your member may be difficult and expensive after the transaction has concluded, you should consider implementing appropriate measures to provide the

consumer with a reasonable opportunity to opt out in the course of that transaction, for example, during the application process.

E. Designing Your Privacy Notices for New Members

The measures discussed in this section may assist you in designing and delivering your initial and annual notices regarding your privacy policy and practices for a new member. The hypothetical transaction is just an example. The transaction you conduct may involve other facts that may require additional measures to comply with the consumer privacy rule.

1. Individual Who Joins Your Credit Union in Person

When an individual becomes a member of your credit union, you must give an initial notice of your privacy policy and practices not later than the time when he or she becomes a member. You satisfy the requirement to provide the notice in writing so that the member can retain or obtain it at a later time if you hand-deliver a printed copy. You may find the simplest way to design the initial notice is to incorporate it directly into the membership agreement or other documents that create the member relationship. This may streamline your delivery method, especially if you do not disclose any nonpublic personal information to nonaffiliated third parties (other than as authorized by an exception) and, therefore, need not provide the member with an opportunity to opt out.

If you design your initial notice as a separate document, then you should establish procedures so that your employee hand-delivers the notice together with documents necessary to become a member. For instance, you may provide the initial notice when the individual first obtains information about credit union membership. Your employees may explain and address questions about your privacy policy and practices, such as whether the member may opt out at a later time. You may not provide any notice required by the consumer privacy rule solely by orally explaining it to the member.

If a member and a nonmember open a joint share draft account, then you may provide one printed copy of the initial notice to those individuals jointly not later than the time when the nonmember's member relationship begins. If you provide the opt out notice to only one of the joint account holders, however, then you must permit that individual to opt out on behalf of both of them.

Regardless of its form, the notice must be clear and conspicuous. If you incorporate the notice into the membership agreement, then you must design the combined document so the privacy notice is distinct from the other provisions of the agreement. For instance, you may use different type size, style, and other graphic devices so the individual is alerted to the privacy notice. If you disclose nonpublic personal information to nonaffiliated third parties, other than as authorized by an exception, then you must design the notice to call the individual's attention to the nature

and significance of the right to opt out of that disclosure. You may make the notice reasonably understandable through a variety of measures, including:

- describing your policy in short explanatory sentences;
- presenting different aspects of your privacy policy in separate sections; and
- avoiding highly technical business terms to explain the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, if applicable.

Your initial and annual notices should accurately describe your privacy policy and practices with respect to all of your products and services. For instance, if a member of your credit union received the last annual notice that also covers your loan products, then you need not provide another initial notice when he or she obtains a loan from you.

2. Individual Who Applies for Membership Through Your Web Site

To provide a notice on your web site, you may consider a mechanism that requires the consumer to acknowledge that he or she agrees to receive the notice electronically as a necessary step to the application process. Alternatively, when you solicit the consumer's electronic mail address you should consider including a provision that seeks the consumer's agreement to receive the notice electronically.

Like the printed copies of your notices, the notices that you provide electronically must be clear and conspicuous. Many of the techniques that you use to design printed notices apply equally to electronic notices, including describing your policy in short explanatory sentences and avoiding highly technical business terms to explain the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information. You also should consider using distinctive graphics to draw the viewer's attention to the notice.

You should take steps to provide the individual with an opportunity to opt out of any disclosures at the time that he or she applies for membership because communicating with him or her later may be difficult and expensive. You could, for instance, provide an opt out notice on a web page that clearly and conspicuously displays check-off boxes as part of the online application itself.

If you extend membership to the individual, and he or she then becomes your member, you may consider delivering your annual notices electronically. To do so, you should take steps to obtain the member's agreement to receive the notice electronically, as discussed above. If the member uses your web site to access his or her account, you could post your current privacy notice continuously in a clear and conspicuous manner on the web site. You should take steps to update the site regularly and ensure that the notice, or a link to the notice, does, in fact, appear continuously in a clear and conspicuous manner on a web page that members frequently access.