

---

# PRIVACY OF CONSUMER FINANCIAL INFORMATION

## OVERVIEW

---

### Overview

Title V, Subtitle A of the Gramm-Leach-Bliley Act (the “GLB Act”) governs the treatment of nonpublic personal information about consumers by financial institutions. Section 502 of Subtitle A, 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.

As required by law, the federal banking agencies, NCUA, the Secretary of the Treasury, the Securities and Exchange Commission, the Federal Trade Commission, and the Commodity Futures Trading Commission, in consultation with state insurance authorities, prescribed regulations “consistent and comparable” with one another. Part 716 of the NCUA Rules and Regulations implements provisions of the Act governing the privacy of consumer financial information for federally insured credit unions. The regulation contains many defined terms (in quotes below; see Glossary), establishes rules governing a credit union’s duties to provide particular notices, and limits its disclosure of nonpublic personal information, as summarized below:

- A credit union must provide a notice of its privacy policies, and allow a “consumer” to opt out of the disclosure of his or her “nonpublic personal information,” to a “nonaffiliated third party” if the disclosure is outside of the exceptions in NCUA Rules and Regulations §716.13, §716.14 or §716.15;
- Regardless of whether a credit union shares “nonpublic personal information,” the credit union must provide notices of its privacy policies to its “members.” Note this term includes some nonmembers for purposes of this rule (see Glossary);
- A credit union generally may not disclose account numbers to any “nonaffiliated third party” for marketing purposes; and,
- A credit union must follow reuse and redisclosure limitations on any nonpublic personal information it receives from a nonaffiliated financial institution.

### Exceptions

Credit unions need not give opt-out notices if the credit unions limit disclosure of nonpublic personal information as follows:

- To a nonaffiliated third party to perform services for the credit union or to function on its behalf, including marketing the credit unions own products or services or those offered jointly by the credit union and another financial institution. This 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. If the service is covered by the exceptions in §716.14 or §716.15, the credit union does not have to comply with the additional disclosure and confidentiality requirements of §716.13. Disclosure under §716.13 could include sharing information for marketing purposes with an insurance company (§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 (§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 (§716.15).

## Associated Risks

- Compliance risk can occur when the credit union fails to implement the necessary controls to comply with the GLB Act and Part 716.
- Reputation risk can occur when members of the credit union learn of its failure to comply with the GLB Act and Part 716.

## Additional Information

- Part 716 is available on NCUA's website in the Reference Information section under Rules and Regulations, [http://www.ncua.gov/ref/rules\\_and\\_regs/NCUA4.pdf](http://www.ncua.gov/ref/rules_and_regs/NCUA4.pdf).
- NCUA's website in the Reference Information section under Consumer Privacy, [http://www.ncua.gov/ref/consumer\\_privacy/consumerprivacy.htm](http://www.ncua.gov/ref/consumer_privacy/consumerprivacy.htm), contains the following documents: [Frequently Asked Questions for the Consumer Privacy Regulation](#); [Consumer Privacy Brochure](#), "Privacy Choices for Your Personal Financial Information;" [Privacy of Consumer Financial Information: Small Credit Union Compliance Guide](#); and [NCUA Letter to Credit Unions No. 02-CU-02](#), NCUA's Privacy of Consumer Financial Information Examination Program.
- The FFIEC website contains an InfoBase on Financial Privacy at <http://www.ffiec.gov/exam/infobase.htm>.

- **The FTC website contains a link called Gramm-Leach-Bliley Act: Financial Privacy, Safeguards, and Pretexting,**  
<http://www.ftc.gov/privacy/glbact/index.html>.

---

# PRIVACY OF CONSUMER FINANCIAL INFORMATION

## OPERATIONAL REQUIREMENTS

---

### Disclosures / Notices

#### Initial Privacy Notice to Consumers [§716.4]

Notices must be clear and conspicuous and accurately reflect the credit union's privacy policies and practices and must be provided prior to the consumer providing any information. Notices are only required for consumers who are not members when the credit union is sharing the collected information with nonaffiliated third parties. 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.

#### Special Rule for Loans [§716.4(f)(2)]

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 the nonpublic personal information with nonaffiliated third parties other than as allowed under the exceptions. Credit unions may provide annual notices to the co-borrowers and guarantors jointly.

#### Initial Privacy Notice to Members [§716.4]

The notice must be clear and conspicuous and accurately reflect the credit union's privacy policies and practices to all members not later than when the member relationship is established. The following is a list of disclosures regarding nonpublic personal information that credit unions must provide in their privacy notices, as applicable:

- Categories of information collected;
- Categories of information disclosed;
- Categories of affiliates and nonaffiliated third parties to whom the credit union may disclose information;
- Policies with respect to the treatment of former members' information;
- Information disclosed to service providers and joint marketers (§ 716. 13);
- An explanation of the opt out right and methods for opting out;
- Any opt out notices the credit union must provide under the Fair Credit Reporting Act with respect to affiliate information sharing;
- Policies for protecting the security and confidentiality of information (see also §748.0 and Part 748, App. A); and

- A statement that the credit union makes disclosures to other nonaffiliated third parties as permitted by law under §716.14 and §716.15.

Subsequent notice is permitted when:

- The member relationship is not established at the member's election (i.e. in the case of a credit union acquiring the consumer's account through a purchase or merger).
- To do otherwise would substantially delay the member's transaction, and the member agrees to the subsequent delivery (i.e. in the case of a student loan or establishing the account by telephone).

Subsequent disclosures must be provided within a reasonable time after establishing a member relationship.

#### Simplified Privacy Notice [§716.6(e)(5)]

If the credit union shares information only under the exceptions available under 716.14 and 716.15, the privacy notice must include the following:

- A statement to this effect;
- Categories of nonpublic personal information it collects;
- Policies and practices the credit union uses to protect the confidentiality and security of nonpublic personal information (see also §748.0 and Part 748 App. A); and,
- A general statement that the credit union makes disclosures to other nonaffiliated third parties as permitted by law.

#### Short-Form Initial Privacy Notice with Opt Out Notice [§716.6(c)]

The notice must be clear and conspicuous and state that the credit union's full privacy notice is available on request. It must also explain a reasonable means by which the consumer may obtain the notice.

A reasonable means might include a toll-free telephone number the consumer may call to request the notice, or for the consumer who conducts business in person, having copies available to provide immediately by hand.

#### Annual Privacy Notice to Members [§716.5]

Notices must be clear and conspicuous and accurately reflect the credit union's privacy policies and practices and must be provided at least once in any period of 12 consecutive months.

### Revised Privacy Notices [§716.8]

When a new category of nonpublic personal information is shared or information with a new category of nonaffiliated party is shared, a revised notice and new opt out notice must be given to members.

### Opt out Notice to Consumers [§716.7]

- The opt out notice must state:
  - (a) That the credit union discloses or reserves the right to disclose nonpublic personal information about the consumer to a nonaffiliated third party;
  - (b) That the consumer has the right to opt out of that disclosure; and,
  - (c) A reasonable means by which the consumer may opt out.
- The information concerning the consumer's right to opt out must include:
  - (a) All categories of nonpublic personal information the credit union discloses or reserves the right to disclose;
  - (b) All categories of nonaffiliated third parties to whom the information is disclosed;
  - (c) That the consumer has the right to opt out of the disclosure of that information; and,
  - (d) The financial products or services to which the opt out direction would apply.
- The credit union should comply with the consumer's direction to opt out as soon as is reasonably practicable.
- Consumers must be allowed to opt out at any time.
- The credit union must continue to honor the consumer's opt out direction until revoked by the consumer in writing (or electronically if the consumer agrees).
- Opt out directions should be honored even after the member relationship ends.

### Delivery Methods

The following are examples of "reasonable means" for delivery (§716.9):

- Hand-delivery of a printed copy;
- Mailing a printed copy to the last known address of the consumer;
- 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; or,

- 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.

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 services electronically.

For annual notices, if the member uses the credit union's web site to access products and services electronically and agrees to receive notices at the web site, the credit union may continuously post the current privacy notice on the web site in a clear and conspicuous manner.

### Limits on Disclosure

If the information is obtained under §716.14 or §716.15, the credit union must refrain from using or disclosing the information except:

- To disclose the information to the affiliates of the financial institution from which it received the information;
- To disclose the information to its own affiliates, which are in turn limited by the same disclosure and use restrictions as the credit union; and,
- 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.

If the information is obtained from a nonaffiliated financial institution other than under one of the exceptions in §716.14 or §716.15, the credit union should refrain from disclosing the information except:

- To the affiliates of the financial institution from which it received the information;
- To its own affiliates, which are in turn limited by the same disclosure restrictions as the credit union; and,
- 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.

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.

## **Recordkeeping**

There are no record retention requirements mentioned in the privacy regulation. However, a credit union would need to produce evidence to support their defense resulting from allegations of prohibited practices, by NCUA or a consumer. NCUA recommends the credit union retain evidence of compliance for one examination cycle and one audit cycle.

## **Enforcement / Liability**

### Administrative Enforcement Authority

NCUA has authority to enforce compliance with the GLB Act and Part 716 for federal credit unions and federally insured credit unions. The FTC has authority to enforce compliance with the GLB Act and FTC's consumer privacy rules for non-federally insured credit unions. If CUSOs are providing consumers with financial products or services, they will also be subject to consumer privacy rules, to be enforced by each federal functional regulator.

### Penalties and Liabilities

There are no civil liability provisions in the regulation; however, state law may provide a basis for an individual to sue the credit union for compliance problems.

### Relation to State Law [§716.17]

Parties may petition the Federal Trade Commission for a determination, after consultation with NCUA and the other financial regulators, that a state statute, regulation, order, or interpretation is not inconsistent with the GLB Act and consumer privacy regulations. The FTC will then determine, in general, that either the federal or state law or provisions of both apply. See the FTC website link for more information on these preemption issues, <http://www.ftc.gov/privacy/glbact/index.html#Preemption>.