

7535-01-U

**NATIONAL CREDIT UNION ADMINISTRATION**

**12 CFR Parts 717, 748**

**Fair Credit Reporting – Proper Disposal of Consumer Information under the Fair and Accurate Credit Transactions Act of 2003**

**AGENCY:** National Credit Union Administration (NCUA).

**ACTION:** Notice of Proposed Rulemaking.

**SUMMARY:** The NCUA Board is requesting comment on a proposal to implement section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) by amending the fair credit reporting and security program regulations and NCUA's Guidelines for Safeguarding Member Information. The proposal would require federal credit unions (FCUs) to develop, implement, and maintain appropriate measures to properly dispose of consumer information derived from consumer reports. FCUs are expected to implement these measures consistent with the provisions in NCUA's Guidelines for Safeguarding Member Information.

**DATES:** Comments must be received by July 12, 2004.

**ADDRESSES:** You may submit comments by any of the following methods:

- Federal eRulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- NCUA Web site: [http://www.ncua.gov/RegulationsOpinionsLaws/proposed\\_regs/proposed\\_regs.html](http://www.ncua.gov/RegulationsOpinionsLaws/proposed_regs/proposed_regs.html). Follow the instructions for submitting comments.
- E-mail: [regcomments@ncua.gov](mailto:regcomments@ncua.gov). Include "FACT Act Disposal Rule" in the subject line of the message.
- FAX: Becky Baker, Secretary of the Board, (703) 518-6319, use the subject line described above for e-mail.
- Mail: Becky Baker, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314-3428.
- Hand Delivery / Courier: Guard station in lobby of 1775 Duke Street, Alexandria, Virginia, on business days between 8:00 a.m. and 5:00 p.m.

Instructions: All submissions received must include the agency name for this rulemaking. Commenters are encouraged to use the title "FACT Act Disposal Rule" to facilitate the organization of comments. **Whatever method you choose, please send comments by one method only.**

**FOR FURTHER INFORMATION CONTACT:** Chrisanthy J. Loizos, Staff Attorney, Office of General Counsel, National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428 or telephone: (703) 518-6540.

## **SUPPLEMENTARY INFORMATION:**

### **I. Introduction**

Section 216 of the FACT Act adds a new section 628 to the Fair Credit Reporting Act (FCRA) that, in general, is designed to protect a consumer against the risks associated with unauthorized access to information about the consumer contained in a consumer report, such as fraud and identity theft.

15 U.S.C. 1681w. Section 216 of the FACT Act requires NCUA to adopt a rule requiring any FCU “that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation.” Pub. L. 108-159, 117 Stat. 1985-86. The FACT Act mandates that the rule be consistent with the requirements issued pursuant to the Gramm-Leach-Bliley Act (GLBA) (Pub. L. 106-102), as well as other provisions of federal law.

NCUA proposes amendments to the fair credit reporting and security program rules and its Guidelines for Safeguarding Member Information, to require FCUs to implement controls designed to ensure the proper disposal of consumer information within the meaning of section 216. 12 CFR parts 717 and 748. In accordance with section 216, NCUA has consulted with the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), Federal Trade Commission (FTC), and Securities and Exchange Commission (collectively, the Agencies) to ensure that, to the extent possible, the rules proposed by the respective agencies to implement section 216 are consistent and comparable. NCUA’s proposed regulation and the preamble are substantively similar to a joint notice of proposed rulemaking that NCUA anticipates will be issued by the federal banking agencies (FRB, OCC, FDIC and OTS) shortly.

### **II. Background**

In 2001, NCUA amended the security program rule to establish standards for federally insured credit unions (FICUs) relating to administrative, technical, and physical safeguards to protect the security and confidentiality of member records and information, pursuant to section 501 of GLBA. 15 U.S.C. 6805(b). NCUA worked with the Agencies and state insurance authorities to develop appropriate standards. 66 FR 8152 (Jan. 30, 2001). The federal banking agencies issued their standards as guidelines under Section 39 of the Federal Deposit Insurance

Act. 12 U.S.C. 1831p.<sup>1</sup> NCUA determined it could best meet the congressional directive to prescribe standards by amending the rule governing security programs and by providing guidance in an appendix to the rule. 12 CFR part 748, Appendix A; 66 FR 8152 (Jan. 30, 2001).

Section 748.0 requires an FICU to develop a security program that implements safeguards designed to: (1) ensure the security and confidentiality of member records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to a member. 12 CFR §748.0(b)(2).

Appendix A to part 748 sets forth NCUA's Guidelines for Safeguarding Member Information (Guidelines), which are substantially identical to the guidelines issued by the Agencies. 66 FR 8152 (Jan. 30, 2001). The Guidelines "are intended to outline industry best practices and assist credit unions to develop meaningful and effective security programs to ensure their compliance with the safeguards contained in the regulation." Id.

The Guidelines direct FICUs to assess the risks to their member information and member information systems and, in turn, implement appropriate security measures to control those risks. 12 CFR part 748, Appendix A. For example, under the risk-assessment framework, FICUs should evaluate whether the controls the FICU has developed sufficiently protect its member information from unauthorized access, misuse, or alteration when the FICU disposes of the information. "[A] credit union's responsibility to safeguard member information continues through the disposal process." 66 FR 8152, 8155.

### **III. Proper Disposal of Consumer Information and Member Information**

Section 216 of the FACT Act requires NCUA to issue final regulations for entities under its enforcement authority under section 621 of the FCRA. Unlike the current provisions in the security program rule, which apply to all FICUs, the requirements in the proposed rule would apply solely to FCUs. See 15 U.S.C. 1681s(b)(3). Federally insured state-chartered credit unions are subject to the enforcement jurisdiction of the FTC for purposes of the FCRA. See 15 U.S.C. 1681s(a). State charters, therefore, should refer to the proposed rule issued by the FTC regarding the proper disposal of consumer information under section 216. 69 FR 21388 (Apr. 20, 2004).

---

<sup>1</sup> 12 CFR parts 30, app. B; 208, app. D-2 and 225, app. F; 364, app. B; 570, app. B. See 66 FR 8616 Feb. 1, 2001.

The NCUA Board proposes to implement section 216 by adding §717.83 to NCUA's fair credit reporting rule<sup>2</sup> that will require FCUs to develop and maintain, as part of their information security programs, appropriate controls designed to ensure that they properly dispose of consumer information. The Board proposes to place a cross-reference in the security program rule, §748.0, that directs FCUs to §717.83 to ensure that controls for the disposal of consumer information are included in FCU information security programs. Lastly, the Board proposes to amend the Guidelines to address the disposal of consumer information. FCUs are expected to dispose of consumer information in a manner consistent with the disposal of member information in the Guidelines.

### Section 717.83 – Disposal of Consumer Information

NCUA proposes to incorporate the new disposal requirement in §717.83 by defining “consumer information” and requiring FCUs to properly dispose of consumer information in a manner consistent with the Guidelines. Proposed §717.83 also incorporates a rule of construction that closely tracks the terms of section 628(b) of the FCRA, as added by section 216 of the FACT Act. It states that the section does not impose any requirements to maintain or destroy consumer records beyond those imposed by any other law. The proposed rule also would not affect any requirement to maintain or destroy consumer records imposed under any other provision of law.

#### **Consumer information**

Section 717.83(d)(1) would define “consumer information” to mean “any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the credit union for a business purpose.” “Consumer information” would also be defined to mean “a compilation of such records.”

The scope of information covered by the terms “consumer information,” and “member information” as defined under the Guidelines, will sometimes overlap, but will not always coincide. NCUA notes that the proposed definition of “consumer information” is drawn from the term “consumer” in section 603(c) of the FCRA, which defines a “consumer” as an individual. 15 U.S.C. 1681a(c). By contrast, “member information” under the Guidelines, only covers nonpublic personal information about a “member,” as defined in §716.3(n), namely, an individual who obtains a financial product or service to be used primarily for personal, family, or household purposes and who has a continuing relationship with the FCU.

---

<sup>2</sup> On April 8, 2004, NCUA proposed a new part 717, implementing section 411 of the FACT Act. See 69 FR 23380 (Apr. 28, 2004).

The relationship between consumer information and member information can be illustrated through the following examples. Payment history information from a consumer report about an individual, who is an FCU's member, will be both consumer information because it comes from a consumer report and member information because it is nonpublic personal information about a member. In some circumstances, member information will be broader than consumer information. For instance, information that an FCU maintains about its member's transactions with the FCU would be only member information because it does not come from a consumer report. In other circumstances, consumer information will be broader than member information. Consumer information would include information from a consumer report that an FCU obtains about an individual who guarantees a loan for a business entity or who has applied for employment with the FCU. In these instances, the consumer reports would not be member information because the information would not be about a "member" within the meaning of the Guidelines but would be consumer information.

NCUA proposes to define "consumer information" as "any record about an individual . . . that is a consumer report or is derived from a consumer report." Under this definition, information that may be "derived from consumer reports" but does not identify a particular consumer would not be covered under the proposed rule. For example, an FCU must implement measures to properly dispose of consumer information that identifies a consumer, such as the consumer's name and the credit score derived from a consumer report. This requirement, however, would not apply to the mean credit score that is derived from a group of consumer reports. NCUA believes that limiting "consumer information" to information that identifies a consumer is consistent with the current law relating to the scope of the term "consumer report" under the FCRA and the purposes of section 216 of the FACT Act.

NCUA requests suggestions for clarifying the scope of the individuals and information covered under the term "consumer information." Among other issues, NCUA believes that the phrase "derived from consumer reports" covers all of the information about a consumer taken from a consumer report, including information that results in whole or in part from manipulation of information from a consumer report or information from a consumer report that has been combined with other types of information. Consequently, an FCU that possesses any of this information must properly dispose of the information.

For example, any record about a consumer derived from a consumer report, such as the consumer's name and credit score, that is shared with an affiliate credit union service organization must be disposed of properly by each affiliate that possesses that information. Similarly, a consumer report that is shared among affiliates after the consumer has been given a notice and has elected not to opt out of that sharing, and therefore is no longer a "consumer report" under

the FCRA<sup>3</sup>, would still be “consumer information” under this proposal. Accordingly, an FCU that receives consumer information under these circumstances must properly dispose of the information. NCUA seeks comment on whether the definition of “consumer information” should be revised to further clarify this interpretation of the statutory phrase “derived from consumer reports,” such as by example or otherwise.

NCUA notes that the proposed definition of “consumer information” includes the qualification “for a business purpose” in section 216 of the FACT Act. NCUA believes that the phrase “for a business purpose” encompasses any commercial purpose for which an FCU might maintain or possess consumer information and requests comment on that interpretation.

## **Compliance**

NCUA proposes to require each FCU to implement the appropriate measures to properly dispose of consumer information within three months after the final rule is published in the Federal Register. NCUA believes that any changes to an FCU’s existing information security program to properly dispose of consumer information likely will be minimal. Accordingly, NCUA considers a three-month period sufficient to enable FCUs to adjust their systems and controls.

### Section 748.0 – Security Program

NCUA proposes to add paragraph (c) to §748.0 to include a cross-reference to the section 216 requirement in §717.83, for ease of reference when FCUs adopt or modify their security programs.

### Guidelines for Safeguarding Member Information

The Board proposes to amend the Guidelines to specifically address the disposal of consumer information by: (1) defining “consumer information” as defined in §717.83; (2) adding an objective regarding the proper disposal of consumer information; and (3) providing that an FCU should implement appropriate measures to properly dispose of consumer information in a manner consistent with the disposal of member information.

### **New Objective for an Information Security Program**

NCUA proposes to add a new objective regarding the proper disposal of consumer information in paragraph II.B. of the Guidelines. The new objective provides that an FCU should design its information security program to “[e]nsure

---

<sup>3</sup> 15 U.S.C. 1681a(d)(2)(A)(iii).

the proper disposal of consumer information in a manner consistent with the disposal of member information.”

By including this additional objective in paragraph II.B., NCUA expects FCUs to review the measures taken by their service providers to properly dispose of consumer information. FCUs should require service providers to develop appropriate measures for the proper disposal of consumer information and, where warranted, monitor service providers to confirm that they have satisfied their contractual obligations. Paragraph III.D.2. of the Guidelines currently provide that a credit union should require “[i]ts service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines.”

NCUA also proposes to amend paragraph III.G.2. to allow an FCU a reasonable period of time, after the final regulations are issued, to amend its contracts with its service providers to incorporate the necessary requirements in connection with the proper disposal of consumer information. NCUA proposes that FCUs modify the contracts that will be affected by the newly-implemented requirements within one year after publication of the final regulations. NCUA seeks comment on whether a one-year period for modification of agreements with service providers is appropriate.

### **New Provision to Implement Measures to Properly Dispose of Consumer Information**

NCUA proposes to amend paragraph III.C. of the Guidelines by adding a new provision stating that an FCU, as part of its information security program, should develop, implement, and maintain, appropriate measures to properly dispose of consumer information. This new provision also provides that FCUs should implement these measures “in a manner consistent with the disposal of member information” and “in accordance with the provisions in paragraph III” of the Guidelines.

Paragraph III of the Guidelines presently states that an FCU should undertake measures to design, implement, and maintain its information security program to protect member information and member information systems, including the methods it uses to dispose of member information. Under the proposal, an FCU is expected to adopt a comparable set of procedures and controls to properly dispose of consumer information. For example, an FCU should broaden the scope of its risk assessment to include an assessment of the reasonably foreseeable internal and external threats associated with the methods it uses to dispose of consumer information, and adjust its risk assessment in light of the relevant changes relating to such threats. By expressly adding this new provision in §748.0(c) and to the Guidelines, NCUA expects FCUs to integrate

into their information security programs the risk-based measures in paragraph III of the Guidelines for the disposal of consumer information.

NCUA believes that it is not necessary to propose a prescriptive rule describing proper methods of disposal. Nonetheless, consistent with interagency guidance previously issued through the Federal Financial Institutions Examination Council (FFIEC),<sup>4</sup> NCUA expects FCUs to have appropriate disposal procedures for records maintained in paper-based or electronic form. NCUA notes that an FCU's information security program should ensure that paper records containing either member or consumer information should be rendered unreadable as indicated by the FCU's risk assessment, such as by shredding or any other means. FCUs also should recognize that computer-based records present unique disposal problems. Residual data frequently remains on media after erasure. Since that data can be recovered, FCUs should apply additional disposal techniques to sensitive electronic data.<sup>5</sup>

NCUA seeks comment on whether the proposed amendment to paragraph III.C. of the Guidelines sufficiently explains the nature and scope of the obligations on FCUs to modify their information security programs, including measures that should be implemented and adjusted, as appropriate, to properly dispose of consumer information.

NCUA also requests comment on whether the use in the proposal of the statutory phrase "proper disposal" is sufficiently clear. Would a more specific standard provide better guidance to FCUs or better protect consumers, or both?

The proposed changes to the Guidelines are intended to provide guidance to FCUs for compliance with proposed §717.83. As noted above, the requirements of this proposed disposal rule only apply to FCUs, while federally insured state-chartered credit unions are subject to the jurisdiction of the FTC on this matter. The Board believes, however, that federally insured state charters may find this guidance helpful in adopting meaningful and effective security programs that deal with the disposal of consumer information.

NCUA invites comment on all aspects of the proposal.

### Comment Period

Generally, NCUA Board's policy is to give the public at least 60 days to comment on a proposed regulation. NCUA Interpretive Ruling and Policy Statement (IRPS) 87-2 (as amended by IRPS 03-2). The Board is issuing this Notice of Proposed Rulemaking with a comment period of 45 days so that the receipt of

---

<sup>4</sup> See FFIEC Information Security Booklet, page 63 at: [http://www.ffiec.gov/ffiecinfobase.html\\_pages/it\\_01.html#infosec](http://www.ffiec.gov/ffiecinfobase.html_pages/it_01.html#infosec).

<sup>5</sup> See footnote 4, *supra*.



comments and issuance of a final rule is as closely timed with the rules issued by the Agencies as possible. The shortened comment period will allow NCUA to issue a final rule by December 4, 2004, as required by section 216. 15 U.S.C. 1681w(a)(1).

#### **IV. Regulatory Procedures**

##### Regulatory Flexibility Act

The Regulatory Flexibility Act requires NCUA to prepare an analysis to describe any significant economic impact any proposed regulation may have on a substantial number of small entities (those under \$10 million in assets). The NCUA Board has determined and certifies that the proposed amendments, if adopted, will not have a significant economic impact on a substantial number of small credit unions. Accordingly, a regulatory flexibility analysis is not required.

The proposed rule would require an FCU to implement appropriate controls designed to ensure the proper disposal of consumer information. An FCU would be required to develop and maintain these controls as part of implementing its existing information security program as required by §748.0.

Any modifications to an FCU's information security program needed to address the proper disposal of consumer information could be incorporated through the process the FCU presently uses to adjust its program under paragraph III.E. of the Guidelines, particularly because of the similarities between the consumer and member information and the measures commonly used to properly dispose of both types of information. To the extent these proposed rules impose new requirements for certain types of consumer information, developing appropriate measures to properly dispose of that information likely would require only a minor modification of an FCU's existing information security program.

Because some consumer information will be member information and because segregating particular records for special treatment may entail considerable costs, NCUA believes that many FCUs, including small entities, already are likely to have implemented measures to properly dispose of both member and consumer information. In addition, NCUA and the federal banking agencies, through the Federal Financial Institutions Examination Council (FFIEC), already have issued guidance regarding their expectations concerning the proper disposal of all of an institution's paper and electronic records. See FFIEC Information Security Booklet, December 2002, p. 63.<sup>6</sup> Therefore, the proposed rules do not require any significant changes for FCUs that currently have procedures and systems designed to comply with this guidance.

---

<sup>6</sup> The FFIEC Information Security Booklet is available at:  
[http://www.ffiec.gov/ffiecinfobase/html\\_pages/it\\_01.html#infosec](http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec).

NCUA anticipates that, in light of current practices relating to the disposal of information in accordance with §748.0, the Guidelines, and the guidance issued by the FFIEC, the proposed rule would not impose undue costs on FCUs. NCUA believes that the controls that small FCUs would need to develop and implement, if any, to comply with the proposed rules likely pose a minimal economic impact on those entities. Nonetheless, NCUA specifically seeks comment on the likely burden the proposed rules would have on small FCUs, and how the proposed rule might minimize this burden, to the extent consistent with the requirements of the FACT Act.

#### Paperwork Reduction Act

NCUA has determined that the proposed regulation does not increase paperwork requirements under the Paperwork Reduction Act of 1995 and regulations of the Office of Management and Budget.

#### Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their regulatory actions on state and local interests. In adherence to fundamental federalism principles, NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. This proposed rule would not have substantial direct effects on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined that the proposed rule does not constitute a policy that has federalism implications for purposes of the executive order.

#### The Treasury and General Government Appropriations Act, 1999 - - Assessment of Federal Regulations and Policies on Families

NCUA has determined that this proposed rule will not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Pub. L. 105-277, 112 Stat. 2681 (1998).

#### Agency Regulatory Goal

NCUA's goal is to promulgate clear and understandable regulations that impose minimal regulatory burden. We request your comments on whether the proposed rule is understandable and minimally intrusive if implemented as proposed.

#### **12 CFR Part 717**

Credit unions, Reporting and recordkeeping requirements.

## **12 CFR Part 748**

Credit unions, Crime, Currency, Reporting and recordkeeping requirements, and Security measures.

By the National Credit Union Administration Board on May 20, 2004.

---

Becky Baker

Secretary of the Board

For the reasons stated in the preamble, NCUA proposes to amend 12 CFR chapter VII as set forth below:

### **PART 717 -- FAIR CREDIT REPORTING**

1. The authority citation for part 717 is revised to read as follows:  
**Authority:** 15 U.S.C. 1681a, 1681s, 1681w, 6801 and 6805(b).

2. Add a new subpart I to read as follows:

Subpart I – Duties of Users of Consumer Reports Regarding Identity Theft

**§717.80-82** [Reserved]

#### **§717.83 Disposal of consumer information.**

(a) In general. You must properly dispose of any consumer information that you maintain or otherwise possess in a manner consistent with the Guidelines for Safeguarding Member Information, in appendix A to part 748 of this chapter.

(b) Rule of construction. Nothing in this section:

- (1) Requires you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or
- (2) Alters or affects any requirement imposed under any other provision of law to maintain or destroy such a record.

(c) Definitions. As used in this section:

(1) Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the credit union for a business purpose. Consumer information also means a compilation of such records.

(2) Consumer report has the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681a(d).

**PART 748 – SECURITY PROGRAM, REPORT OF CRIME AND CATASTROPHIC ACT AND BANK SECRECY ACT COMPLIANCE**

3. The authority citation for Part 748 is revised to read as follows:

**Authority:** 12 U.S.C. 1766(a), 1786(Q); 15 U.S.C. 1681s, 1681w, 6801, and 6805(b); 31 U.S.C. 5311 and 5318.

4. Amend §748.0 by adding paragraph (c) to read as follows:

**§748.0 Security program.**

\* \* \* \* \*

(c) Each federal credit union, as part of its information security program, must properly dispose of any consumer information the federal credit union maintains or otherwise possesses, as required under §717.83 of this part.

5. Amend Appendix A to Part 748 as follows:

a. Add the following sentence at the end of paragraph I.: “These Guidelines also address standards with respect to the proper disposal of consumer information pursuant to sections 621(b) and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s(b) and 1681w).”;

b. Add the following sentence as the end of paragraph I.A.: “These Guidelines also apply to the proper disposal of consumer information by such entities.”;

c. Redesignate paragraphs I.B.2.a. through d. as I.B.2.c. through f.;

d. Add new paragraphs I.B.2.a. and b. to read:

a. Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the credit union for a business purpose. Consumer information also means a compilation of such records.

b. Consumer report has the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681a(d).

e. Amend paragraph II.B. by removing the word “and” after the word “information;” and adding the following phrase after the word “member” at the

end of the sentence: “; and ensure the proper disposal of consumer information in a manner consistent with the disposal of member information”;

f. Add a new paragraph III.C.4. to read as follows:

“4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of consumer information in a manner consistent with the disposal of member information, in accordance with the provisions in paragraph III.”

g. Add paragraphs III.G.3. and III.G.4. to read as follows:

3. Effective date for measures relating to the disposal of consumer information. Each federal credit union must properly dispose of consumer information in a manner consistent with these Guidelines by [This date will be 90 days after the date of publication in the FEDERAL REGISTER of a final rule].

4. Exception for existing agreements with service providers relating to the disposal of consumer information. Notwithstanding the requirement in paragraph III.G.3., a federal credit union’s existing contracts with its service providers with regard to any service involving the disposal of consumer information should implement the objectives of these Guidelines by [This date will be one year after the date of publication in the FEDERAL REGISTER of a final rule].