

Proposed Rules

Federal Register

Vol. 68, No. 210

Thursday, October 30, 2003

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

AGENCY: National Credit Union Administration (NCUA).

ACTION: Notice of proposed rulemaking and request for comment.

SUMMARY: The NCUA Board is proposing a modification to its security program requirements to include response programs for unauthorized access to member information. Further, the NCUA Board is requesting comment on proposed Guidelines for implementing a response program for unauthorized access to member information, including member notice.

In addition, as part of its continuing efforts to reduce paperwork and respondent burden, NCUA invites the general public and other federal agencies to take this opportunity to comment on a proposed information collection, as required by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35).

DATES: Comments must be received on or before December 29, 2003.

ADDRESSES: Direct comments to Becky Baker, Secretary of the Board. Mail or hand deliver comments to: National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428. You are encouraged to fax comments to (703) 518-6319 or email comments to regcomments@ncua.gov instead of mailing or hand-delivering them. Whatever method you choose, *please send comments by one method only.*

FOR FURTHER INFORMATION CONTACT: Matthew J. Biliouris, Senior Information Systems Officer, Office of Examination & Insurance, Division of Supervision, (703) 518-6394.

SUPPLEMENTARY INFORMATION:

I. Background

In 2001, NCUA amended 12 CFR Part 748 to fulfill a requirement in Section 501 of the Gramm-Leach-Bliley Act (GLBA) (Pub. L. 106-102), in which Congress directed NCUA and the federal banking agencies, including the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the "Agencies") to establish standards for financial institutions relating to administrative, technical, and physical safeguards to: (1) Insure the security and confidentiality of customer 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 any customer.¹

Although NCUA worked with the other Agencies to develop the standards described above, the other Agencies issued their standards as guidelines under the authority of Section 39 of the Federal Deposit Insurance Act.

Since Section 39 of the Federal Deposit Insurance Act does not apply to NCUA, the agency determined that it could best meet the congressional directive to prescribe standards through an amendment to its existing regulation governing security programs for federally insured credit unions and provide guidance to credit unions, substantially identical to the guidelines issued by the Agencies, in an appendix to the regulation. 12 CFR Part 748, Appendix A; 66 FR 8152 (January 30, 2001) (the preamble to the final rule discusses the different regulatory framework under which the other federal financial institution regulators issued their guidelines). The final regulation requires that federally insured credit unions establish and maintain a security program implementing the safeguards required by the GLBA.

Appendix A, entitled Guidelines for Safeguarding Member Information, (Appendix A) is intended to outline industry best practices and assist credit unions to develop meaningful and effective security programs to ensure

their compliance with the requirements contained in the regulation. Among other things, Appendix A advises credit unions to: (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and (3) assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.²

This proposed rule further amends Part 748 to require that federally insured credit unions' security programs contain a provision for responding to incidents of unauthorized access to member information. An Appendix B, entitled Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, is also provided to assist credit unions in developing and maintaining their response programs.

As proposed, Appendix B describes NCUA's expectation that every federally insured credit union develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of member information maintained by the credit union or its service provider. Appendix B (referred to hereinafter as the "proposed Guidance") further describes the components of a response program, which should include procedures for notifying members about incidents of unauthorized access to member information that could result in substantial harm or inconvenience to the member. The proposed Guidance provides that a credit union is expected to expeditiously implement its response program to address incidents of unauthorized access to or use of member information. A response program should contain policies and procedures that enable the credit union to:

A. Assess the situation to determine the nature and scope of the incident, and identify the information systems and types of member information affected;

B. Notify the credit union's regulator and, in accordance with applicable

¹ 12 CFR part 748.

² 12 CFR Part 748, Appendix. A, Paragraph III.B.