(4) Provide training for appropriate personnel.

(Approved by the Office of Management and Budget under control number 3133–0094)

[52 FR 2861, Jan. 27, 1987, as amended at 52 FR 8062, Mar. 16, 1987; 68 FR 25112, May 9, 2003]

APPENDIX A TO PART 748—GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

TABLE OF CONTENTS

I. INTRODUCTION

The Guidelines for Safeguarding Member Information (Guidelines) set forth standards pursuant to sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information. 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).

A. *Scope.* The Guidelines apply to member information maintained by or on behalf of federally-insured credit unions. Such entities are referred to in this appendix as ''the credit union.'' These Guidelines also apply to the proper disposal of consumer information by such entities.

B. *Definitions.* 1. *In general.* Except as modified in the Guidelines or unless the context otherwise requires, the terms used in these Guidelines have the same meanings as set forth in 12 CFR part 716.

2. For purposes of the Guidelines, the following definitions apply:

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. The term does not include any record that does not identify an individual.

b. Consumer report has the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681a(d). The meaning of consumer report is broad and subject to various definitions, conditions and exceptions in the Fair Credit Reporting Act. It includes written or oral communications from a consumer reporting agency to a third party of information used or collected for use in establishing eligibility for credit or insurance used primarily for personal, family or household purposes, and eligibility for employment purposes. Examples include credit reports, bad check lists, and tenant screening reports.

c. *Member* means any member of the credit union as defined in 12 CFR 716.3(n).

d. *Member information* means any records containing nonpublic personal information, as defined in 12 CFR 716.3(q), about a member, whether in paper, electronic, or other form, that is maintained by or on behalf of the credit union.

e. *Member information system* means any method used to access, collect, store, use, transmit, protect, or dispose of member information.

f. *Service provider* means any person or entity that maintains, processes, or otherwise is permitted access to member information through its provision of services directly to the credit union.

II. STANDARDS FOR SAFEGUARDING MEMBER INFORMATION

A. *Information Security Program.* A comprehensive written information security program includes administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities. While all parts of the credit union are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. *Objectives.* A credit union's information security program should be designed to: ensure the security and confidentiality of member information; protect against any anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member; and ensure the proper disposal of member information and consumer information. Protecting confidentiality includes honoring members' requests to opt out of disclosures to nonaffiliated third parties, as described in 12 CFR 716.1(a)(3).

III. DEVELOPMENT AND IMPLEMENTATION OF MEMBER INFORMATION SECURITY PROGRAM

A. *Involve the Board of Directors.* The board of directors or an appropriate committee of the board of each credit union should:

1. Approve the credit union's written information security policy and program; and

2. Oversee the development, implementation, and maintenance of the credit union's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. *Assess Risk.* Each credit union should:

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.

C. *Manage and Control Risk.* Each credit union should:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the credit union's activities. Each credit union must consider whether the following security measures are appropriate for the credit union and, if so, adopt those measures the credit union concludes are appropriate:

a. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Access restrictions at physical locations containing member information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that member information system modifications are consistent with the credit union's information security program;

e. Dual controls procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems;

g. Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures.

2. Train staff to implement the credit union's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

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

D. *Oversee Service Provider Arrangements.* Each credit union should:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines; and

3. Where indicated by the credit union's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a credit union should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each credit union should monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its member information, internal or external threats to information, and the credit union's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to member information systems.

F. *Report to the Board.* Each credit union should report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the credit union's compliance with these guidelines. The report should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for

changes in the information security program.

G. *Implement the Standards.*

1. *Effective date.* Each credit union must implement an information security program pursuant to the objectives of these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a credit union has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of paragraph III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of member information, as long as the credit union entered into the contract on or before March 1, 2001.

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 July 1, 2005.

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 July 1, 2006.

[66 FR 8161, Jan. 30, 2001, as amended at 69 FR 69274, Nov. 29, 2004]

APPENDIX B TO PART 748—GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO MEMBER INFORMATION AND MEMBER NOTICE

I. BACKGROUND

This Guidance in the form of Appendix B to NCUA's Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance regulation,[29] interprets section 501(b) of the Gramm-Leach-Bliley Act (''GLBA'') and describes response programs, including member notification procedures, that a federally insured credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. The scope of, and definitions of terms used in, this Guidance are identical to those of Appendix A to Part 748 (Appendix A). For example, the term ''member information'' is the same term used in Appendix A, and means any record containing nonpublic personal information about a member, whether in paper, electronic, or other form, maintained by or on behalf of the credit union.

[29] 12 CFR Part 748.

A. Security Guidelines

Section 501(b) of the GLBA required the NCUA to establish appropriate standards for credit unions subject to its jurisdiction that include administrative, technical, and physical safeguards to protect the security and confidentiality of member information. Accordingly, the NCUA amended Part 748 of its rules to require credit unions to develop appropriate security programs, and issued Appendix A, reflecting its expectation that every federally insured credit union would develop an information security program designed to:

1. Ensure the security and confidentiality of member information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member.

B. Risk Assessment and Controls

1. Appendix A directs every credit union to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of member information; and

c. The sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[30]

2. Following the assessment of these risks, Appendix A directs a credit union to design a program to address the identified risks. The particular security measures a credit union should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the credit union should consider the specific security measures enumerated in Appendix A,[31] and adopt those that are appropriate for the credit union, including:

a. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Background checks for employees with responsibilities for access to member information; and

[30] *See* 12 CFR Part 748, Appendix A, Paragraph III.B.

[31] *See* Appendix A, paragraph III.C.