

National Credit Union Administration

§ 748.0

(3) The presiding officer may order that the hearing be continued for a reasonable period following completion of witness testimony or oral argument to allow additional written submissions to the hearing record.

(4) A Respondent shall bear the burden of demonstrating that his or her continued employment by or service with the credit union would materially strengthen the credit union's ability to—

(i) Become “adequately capitalized,” to the extent that the directive was issued as a result of the credit union's net worth category classification or its failure to submit or implement a net worth restoration plan or revised business plan; and

(ii) Correct the unsafe or unsound condition or unsafe or unsound practice, to the extent that the directive was issued as a result of reclassification of the credit union pursuant to §§702.102(b) and 702.302(d) of this chapter.

(5) Within 20 calendar days following the date of closing of the hearing and the record, the presiding officer shall make a recommendation to the NCUA Board concerning the Respondent's request for reinstatement with the credit union.

(f) *Time for final decision.* Not later than 60 calendar days after the date the record is closed, or the date of the response in a case where no hearing was requested, the NCUA Board shall grant or deny the request for reinstatement and shall notify the Respondent of its decision. If the NCUA Board denies the request for reinstatement, it shall set forth in the notification the reasons for its decision. The decision of the NCUA Board shall be final.

(g) *Effective date.* Unless otherwise ordered by the NCUA Board, the Respondent's dismissal shall take and remain in effect pending a final decision on the request for reinstatement.

§ 747.2005 Enforcement of orders.

(a) *Judicial remedies.* Whenever a credit union fails to comply with a directive imposing a discretionary supervisory action, or enforcing a mandatory supervisory action under part 702 of this chapter, the NCUA Board may seek enforcement of the directive in

the appropriate United States District Court pursuant to 12 U.S.C. 1786(k)(1).

(b) *Administrative remedies—(1) Failure to comply with directive.* Pursuant to 12 U.S.C. 1786(k)(2)(A), the NCUA Board may assess a civil money penalty against any credit union that violates or otherwise fails to comply with any final directive issued under part 702 of this chapter, or against any institution-affiliated party of a credit union (per 12 U.S.C. 1786(r)) who participates in such violation or noncompliance.

(2) *Failure to implement plan.* Pursuant to 12 U.S.C. 1786(k)(2)(A), the NCUA Board may assess a civil money penalty against a credit union which fails to implement a net worth restoration plan under subpart B of part 702 of this chapter or a revised business plan under subpart C of part 702, regardless whether the plan was published.

(c) *Other enforcement action.* In addition to the actions described in paragraphs (a) and (b) of this section, the NCUA Board may seek enforcement of the directives issued under part 702 of this chapter through any other judicial or administrative proceeding authorized by law.

[65 FR 8594, Feb. 18, 2000, as amended at 67 FR 71094, Nov. 29, 2002]

PART 748—SECURITY PROGRAM, REPORT OF CRIME AND CATASTROPHIC ACT AND BANK SECURITY ACT COMPLIANCE

Sec.

748.0 Security program.

748.1 Filing of reports.

748.2 Procedures for monitoring Bank Security Act (BSA) compliance.

APPENDIX A TO PART 748—GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

AUTHORITY: 12 U.S.C. 1766(a), 1786(q); 15 U.S.C. 6801 and 6805(b); 31 U.S.C. 5311 and 5318.

§ 748.0 Security program.

(a) Each federally insured credit union will develop a written security program within 90 days of the effective date of insurance.

(b) The security program will be designed to:

(1) Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;

§ 748.1

(2) Ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

(3) Assist in the identification of persons who commit or attempt such actions and crimes; and

(4) Prevent destruction of vital records, as defined in 12 CFR part 749.

[50 FR 53295, Dec. 31, 1985, as amended at 53 FR 4845, Feb. 18, 1988; 66 FR 8161, Jan. 30, 2001]

§ 748.1 Filing of reports.

(a) *Compliance report.* Each federally insured credit union shall file with the regional director an annual statement certifying its compliance with the requirements of this part. The statement shall be dated and signed by the president or other managing officer of the credit union. The statement is contained on the Report of Officials which is submitted annually by federally insured credit unions after the election of officials. In the case of federally insured state-chartered credit unions, this statement can be mailed to the regional director via the state supervisory authority, if desired. In any event, a copy of the statement shall always be sent to the appropriate state supervisory authority.

(b) *Catastrophic act report.* Each federally insured credit union will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s). A catastrophic act is any natural disaster such as a flood, tornado, earthquake, etc., or major fire or other disaster resulting in some physical destruction or damage to the credit union. Within a reasonable time after a catastrophic act occurs, the credit union shall ensure that a record of the incident is prepared and filed at its main office. In the preparation of such record, the credit union should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has

12 CFR Ch. VII (1-1-04 Edition)

been done or is planned to be done to correct the deficiency(ies).

(c) *Suspicious Activity Report.* (1) Each federally-insured credit union will report any crime or suspected crime that occurs at its office(s), utilizing NCUA Form 2362, Suspicious Activity Report (SAR), within thirty calendar days after discovery. Each federally-insured credit union must follow the instructions and reporting requirements accompanying the SAR. Copies of the SAR may be obtained from the appropriate NCUA Regional Office.

(2) Each federally-insured credit union shall maintain a copy of any SAR that it files and the original of all attachments to the report for a period of five years from the date of the report, unless the credit union is informed in writing by the National Credit Union Administration that the materials may be discarded sooner.

(3) Failure to file a SAR in accordance with the instructions accompanying the report may subject the federally-insured credit union, its officers, directors, agents or other institution-affiliated parties to the assessment of civil money penalties or other administrative actions.

(4) Filing of Suspicious Activity Reports will ensure that law enforcement agencies and NCUA are promptly notified of actual or suspected crimes. Information contained on SARs' will be entered into an interagency database and will assist the federal government in taking appropriate action.

[50 FR 53295, Dec. 31, 1985, as amended at 53 FR 26232, July 12, 1988; 58 FR 17492, Apr. 5, 1993; 61 FR 11527, Mar. 21, 1996]

§ 748.2 Procedures for monitoring Bank Secrecy Act (BSA) compliance.

(a) *Purpose.* This section is issued to ensure that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the requirements of subchapter II of chapter 53 of title 31, United States Code, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act, and the implementing regulations promulgated thereunder by the Department of Treasury, 31 CFR part 103.

(b) *Establishment of a BSA compliance program*—(1) *Program requirement.* Each federally-insured credit union shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and recording requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program must be written, approved by the credit union's board of directors, and reflected in the minutes of the credit union.

(2) *Customer identification program.* Each federally-insured credit union is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the NCUA and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the BSA compliance program required under this section.

(c) *Contents of compliance program.* Such compliance program shall at a minimum—

- (1) Provide for a system of internal controls to assure ongoing compliance;
- (2) Provide for independent testing for compliance to be conducted by credit union personnel or outside parties;
- (3) Designate an individual responsible for coordinating and monitoring day-to-day compliance; and
- (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
 - A. Scope
 - B. Definitions
- II. Guidelines for Safeguarding Member Information
 - A. Information Security Program
 - B. Objectives

- III. Development and Implementation of Member Information Security Program
 - A. Involve the Board of Directors
 - B. Assess Risk
 - C. Manage and Control Risk
 - D. Oversee Service Provider Arrangements
 - E. Adjust the Program
 - F. Report to the Board
 - G. Implement the Standards

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.

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."

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

b. *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.

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

d. *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; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member. 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.

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.

[66 FR 8161, Jan. 30, 2001]

PART 749—RECORDS PRESERVATION PROGRAM AND RECORD RETENTION APPENDIX

Sec.

749.0 What is covered in this part?

749.1 What are vital records?

749.2 What must a credit union do with vital records?

749.3 What is a vital records center?

749.4 What format may the credit union use for preserving records?

749.5 What format may credit unions use for maintaining writings, records or information required by other NCUA regulations?

APPENDIX A TO PART 749—RECORD RETENTION GUIDELINES

AUTHORITY: 12 U.S.C. 1766, 1783 and 1789, 15 U.S.C. 7001(d).

SOURCE: 66 FR 40579, Aug. 3, 2001, unless otherwise noted.

§ 749.0 What is covered in this part?

This part describes the obligations of all federally insured credit unions to maintain a records preservation program to identify, store and reconstruct vital records in the event that the credit union's records are destroyed. It establishes flexibility in the format credit unions may use for maintaining writings, records or information required by other NCUA regulations. The appendix also provides guidance concerning the appropriate length of time credit unions should retain various types of operational records.

§ 749.1 What are vital records?

Vital records include at least the following records, as of the most recent month-end:

(a) A list of share, deposit, and loan balances for each member's account which:

(1) Shows each balance individually identified by a name or number;

(2) Lists multiple loans of one account separately; and

(3) Contains information sufficient to enable the credit union to locate each member, such as address and telephone number, unless the board of directors determines that the information is readily available from another source.

(b) A financial report, which lists all of the credit union's asset and liability accounts and bank reconciliations.

(c) A list of the credit union's financial institutions, insurance policies, and investments. This information may be marked "permanent" and stored separately, to be updated only when changes are made.

§ 749.2 What must a credit union do with vital records?

The board of directors of a credit union is responsible for establishing a vital records preservation program within 6 months after its insurance certificate is issued. The vital records preservation program must contain procedures for storing duplicate vital records at a vital records center and must designate the staff member responsible for carrying out the vital records duties. Records must be stored every 3 months, within 30 days after the end of the 3-month period. Previously stored records may be destroyed when the current records are stored. The credit union must also maintain a records preservation log showing what records were stored, where the records were stored, when the records were stored, and who sent the records for storage. Credit unions, which have some or all of their records maintained by an off-site data processor, are considered to be in compliance for the storage of those records.

§ 749.3 What is a vital records center?

A vital records center is defined as a storage facility at any location far enough from the credit union's offices