

§ 747.3006

§ 747.3006 Conservatorship or liquidation of critically undercapitalized corporate credit union.

Notwithstanding any other provision of this title, the NCUA may, without any administrative due process, immediately place into conservatorship or liquidation any corporate credit union that has been categorized as critically undercapitalized.

PART 748—SECURITY PROGRAM, REPORT OF SUSPECTED CRIMES, SUSPICIOUS TRANSACTIONS, CATASTROPHIC ACTS AND BANK SECRECY ACT COMPLIANCE

Sec.

748.0 Security program.

748.1 Filing of reports.

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

APPENDIX A TO PART 748—GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

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

AUTHORITY: 12 U.S.C. 1766(a), 1786(q); 15 U.S.C. 6801-6809; 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;

(2) Ensure the security and confidentiality of member records, protect against the 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) Respond to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member;

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

12 CFR Ch. VII (1-1-14 Edition)

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

(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 chapter.

[50 FR 53295, Dec. 31, 1985, as amended at 53 FR 4845, Feb. 18, 1988; 66 FR 8161, Jan. 30, 2001; 69 FR 69274, Nov. 29, 2004; 70 FR 22778, May 2, 2005]

§ 748.1 Filing of reports.

(a) The president or managing official of each federally insured credit union must certify compliance with the requirements of this part in its Credit Union Profile annually through NCUA's online information management system.

(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 disaster, natural or otherwise, resulting in physical destruction or damage to the credit union or causing an interruption in vital member services, as defined in § 749.1 of this chapter, projected to last more than two consecutive business days. 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 been done or is planned to be done to correct the deficiency(ies).

(c) *Suspicious Activity Report.* A credit union must file a report if it knows, suspects, or has reason to suspect that any crime or any suspicious transaction related to money laundering activity or a violation of the Bank Secrecy Act has occurred. For the purposes of this paragraph (c) *credit union* means a federally-insured credit union and *official* means any member of the

National Credit Union Administration

§ 748.1

board of directors or a volunteer committee.

(1) *Reportable activity. Transaction* for purposes of this paragraph means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, share certificate, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected. A credit union must report any known or suspected crime or any suspicious transaction related to money laundering or other illegal activity, for example, terrorism financing, loan fraud, or embezzlement, or a violation of the Bank Secrecy Act by sending a completed suspicious activity report (SAR) to the Financial Crimes Enforcement Network (FinCEN) in the following circumstances:

(i) *Insider abuse involving any amount.* Whenever the credit union detects any known or suspected Federal criminal violations, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, where the credit union believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, and the credit union has a substantial basis for identifying one of the credit union's officials, employees, or agents as having committed or aided in the commission of the criminal violation, regardless of the amount involved in the violation;

(ii) *Transactions aggregating \$5,000 or more where a suspect can be identified.* Whenever the credit union detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, and involving or aggregating \$5,000 or more in funds or other assets, where the credit union believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate

a criminal transaction, and the credit union has a substantial basis for identifying a possible suspect or group of suspects. If it is determined before filing this report that the identified suspect or group of suspects has used an alias, then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported;

(iii) *Transactions aggregating \$25,000 or more regardless of potential suspects.* Whenever the credit union detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, involving or aggregating \$25,000 or more in funds or other assets, where the credit union believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, even though the credit union has no substantial basis for identifying a possible suspect or group of suspects; or

(iv) *Transactions aggregating \$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.* Any transaction conducted or attempted by, at or through the credit union and involving or aggregating \$5,000 or more in funds or other assets, if the credit union knows, suspects, or has reason to suspect:

(A) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law;

(B) The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or

(C) The transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular member would normally be expected to engage, and the credit

§ 748.1

12 CFR Ch. VII (1–1–14 Edition)

union knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

(v) *Exceptions.* A credit union is not required to file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities and the credit union files a report pursuant to the reporting requirements of 17 CFR 240.17f-1.

(2) *Filing Procedures.* (i) *Timing.* A credit union must file a SAR with FinCEN no later than 30 calendar days from the date the suspicious activity is initially detected, unless there is no identified suspect on the date of detection. If no suspect is identified on the date of detection, a credit union may use an additional 30 calendar days to identify a suspect before filing a SAR. In no case may a credit union take more than 60 days from the date it initially detects a reportable transaction to file a SAR. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, a credit union must immediately notify, by telephone, an appropriate law enforcement authority and its supervisory authority, in addition to filing a SAR.

(ii) *Content.* A credit union must complete, fully and accurately, SAR form TDF 90-22.47, Suspicious Activity Report (also known as NCUA Form 2362) in accordance with the form's instructions and 31 CFR 1020.320. A copy of the SAR form may be obtained from the credit union resources section of NCUA's Web site, <http://www.ncua.gov>, or the regulatory section of FinCEN's Web site, <http://www.fincen.gov>. These sites include other useful guidance on SARs, for example, forms and filing instructions, Frequently Asked Questions, and the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual.

(iii) *Compliance.* Failure to file a SAR as required by the form's instructions and 31 CFR 1020.320 may subject the credit union, its officials, employees, and agents to the assessment of civil money penalties or other administrative actions.

(3) *Retention of Records.* A credit union must maintain a copy of any SAR that it files and the original or business record equivalent of all supporting documentation to the report for a period of five years from the date of the report. Supporting documentation must be identified and maintained by the credit union as such. Supporting documentation is considered a part of the filed report even though it should not be actually filed with the submitted report. A credit union must make all supporting documentation available to appropriate law enforcement authorities and its regulatory supervisory authority upon request.

(4) *Notification to board of directors.* (i) *Generally.* The management of the credit union must promptly notify its board of directors, or a committee designated by the board of directors to receive such notice, of any SAR filed.

(ii) *Suspect is a director or committee member.* If a credit union files a SAR and the suspect is a director or member of a committee designated by the board of directors to receive notice of SAR filings, the credit union may not notify the suspect, pursuant to 31 U.S.C. 5318(g)(2), but must notify the remaining directors, or designated committee members, who are not suspects.

(5) *Confidentiality of reports.* SARs are confidential. Any credit union, including its officials, employees, and agents, subpoenaed or otherwise requested to disclose a SAR or the information in a SAR must decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed, citing this part, applicable law, for example, 31 U.S.C. 5318(g), or both, and notify NCUA of the request. A credit union must make the filed report and all supporting documentation available to appropriate law enforcement authorities and its regulatory supervisory authority upon request.

(6) *Safe Harbor.* Any credit union, including its officials, employees, and agents, that makes a report of suspected or known criminal violations and suspicious activities to law enforcement and financial institution supervisory authorities, including supporting documentation, are protected from liability for any disclosure in the

report, or for failure to disclose the existence of the report, or both, to the full extent provided by 31 U.S.C. 5318(g)(3). This protection applies if the report is filed pursuant to this part or is filed on a voluntary basis.

[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; 71 FR 62878, Oct. 27, 2006; 72 FR 42273, Aug. 2, 2007; 74 FR 35769, July 21, 2009; 76 FR 18366, Apr. 4, 2011; 78 FR 64885, Oct. 30, 2013]

§ 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 under it by the Department of Treasury, 31 CFR chapter X.

(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 in subchapter II of chapter 53 of title 31, United States Code and implementing regulations issued by the Department of Treasury at 31 CFR chapter X. The compliance program must be written, approved by the credit union's board of directors, and reflected in the credit union's minutes.

(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 Department of the Treasury at 31 CFR 1020.220, 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; 76 FR 18366, Apr. 4, 2011]

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. 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