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.* (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

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.

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

c. 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.[32]

C. Service Providers

Appendix A advises every credit union to require its service providers by contract to implement appropriate measures designed to

[29] 12 CFR Part 748.

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

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

[32] *See* Appendix A, Paragraph III.C.

protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.[33]

II. RESPONSE PROGRAM

i. Millions of Americans, throughout the country, have been victims of identity theft.[34] Identity thieves misuse personal information they obtain from a number of sources, including credit unions, to perpetrate identity theft. Therefore, credit unions should take preventative measures to safeguard member information against such attempts to gain unauthorized access to the information. For example, credit unions should place access controls on member information systems and conduct background checks for employees who are authorized to access member information.[35] However, every credit union should also develop and implement a risk-based response program to address incidents of unauthorized access to member information in member information systems that occur nonetheless.[36] A response program should be a key part of a credit union's information security program.[37] The program should be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

ii. In addition, each credit union should be able to address incidents of unauthorized access to member information in member information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in this Guidance that relate to these arrangements, and with existing guidance on this topic issued by the NCUA,[38] a credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information, including notification of the credit union as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

A. Components of a Response Program

1. At a minimum, a credit union's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused;

b. Notifying the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information as defined below.

c. Consistent with the NCUA's Suspicious Activity Report (''SAR'') regulations,[39] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, for example, by monitoring, freezing, or

[33] *See* Appendix A, Paragraph III.B. and III.D. Further, the NCUA notes that, in addition to contractual obligations to a credit union, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission (ldquo;FTC''), 12 CFR Part 314.

[34] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identify theft in 2002. *See* The Federal Trade Commission, *Identity Theft Survey Report*, (September 2003), available at *http://www.ftc.gov/os/2003/09synovatereport.pdf*.

[35] Credit unions should also conduct background checks of employees to ensure that the credit union does not violate 12 U.S.C. 1785(d), which prohibits a credit union from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1786(g).

[36] Under 12 CFR Part 748, Appendix A, a credit union's *member information systems* consists of all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information, including the systems maintained by its service providers. *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.d.

[37] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December, 2002), available at *http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec*, for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[38] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, (June 2004), available at *http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#outscouring* for additional guidance on managing outsourced relationships.

[39] A credit union's obligation to file a SAR is set out in the NCUA's SAR regulations and guidance. *See* 12 CFR Part 748.1(c); NCUA Letter to Credit Unions No. 04–CU–03, Suspiciouis Activity Reports, March 2004; NCUA Regulatory Alert No. 04–RA–01, The Suspicious Activity Report (SAR) Activity Review—Trends, Tips, & Isues, Issue 6, November 2003, February 2004.

closing affected accounts, while preserving records and other evidence; [40] and

e. Notifying members when warranted.

2. Where an incident of unauthorized access to member information involves member information systems maintained by a credit union's service providers, it is the responsibility of the credit union to notify the credit union's members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

III. MEMBER NOTICE

i. Credit unions have an affirmative duty to protect their members' information against unauthorized access or use. Notifying members of a security incident involving the unauthorized access or use of the member's information in accordance with the standard set forth below is a key part of that duty.

ii. Timely notification of members is important to manage a credit union's reputation risk. Effective notice also may reduce a credit union's legal risk, assist in maintaining good member relations, and enable the credit union's members to take steps to protect themselves against the consequences of identity theft. When member notification is warranted, a credit union may not forgo notifying its customers of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible. Member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay. However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

1. Sensitive Member Information

Under Part 748.0, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member. Substantial harm or inconvenience is most likely to result from improper access to *sensitive member information* because this type of information is most likely to be misused, as in the commission of identity theft.

For purposes of this Guidance, sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. *Sensitive member information* also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

2. Affected Members

If a credit union, based upon its investigation, can determine from its logs or other data precisely which members' information has been improperly accessed, it may limit notification to those members with regard to whom the credit union determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed. If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information is reasonably possible, it should notify all members in the group.

B. Content of Member Notice

1. Member notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of member information that was the subject of unauthorized access or use. It also should generally describe what the credit union has done to protect the members' information from further unauthorized access. In addition, it should include a telephone number that members can call for further information and assistance.[41] The notice also should remind members of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the credit union. The notice should include the following additional items, when appropriate:

a. A recommendation that the member review account statements and immediately

[40] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December 2002), pp. 68–74.

[41] The credit union should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to member inquiries and requests for assistance.

report any suspicious activity to the credit union;

b. A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;

c. A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the member may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.[42]

2. NCUA encourages credit unions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of members that include contact information for the reporting agencies.

C. Delivery of Member Notice

Member notice should be delivered in any manner designed to ensure that a member can reasonably be expected to receive it. For example, the credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically.

[70 FR 22778, May 2, 2005]

PART 749—RECORDS PRESERVATION PROGRAM AND RECORD RETENTION APPENDIX

Sec.

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 reconcilements.

(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.

[42] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.ftc.gov/idtheft* and 1–877–IDTHEFT. The credit union may also refer members to any materials developed pursuant to section 15(1)(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).