7535-01-U

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.

[1] 15 U.S.C. 6805(b).

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

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

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 regulations and guidance, file a Suspicious Activity Report and notify appropriate law enforcement agencies;

C. Take measures to contain and control the incident to prevent further unauthorized access to or use of member information, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls; and

D. Address and mitigate harm to individual members.

The proposed Guidance describes the following corrective measures a credit union should include as a part of its response program in order to effectively address and mitigate harm to individual members:

A. Flag Accounts -- The credit union should identify accounts of members whose information may have been compromised, monitor those accounts for unusual activity, and initiate appropriate controls to prevent the unauthorized withdrawal or transfer of funds from member accounts.

B. Secure Accounts -- The credit union should secure all accounts associated with the member information that has been the subject of unauthorized access or use.

C. Member Notice and Assistance -- The credit union should, under certain circumstances, notify affected members when sensitive member information about them is the subject of unauthorized access. Where the credit union can specifically identify affected members from its logs, notification may be limited to those persons only. Otherwise, the credit union should notify each member in those groups likely to be affected.

The proposed Guidance provides that a credit union should notify each affected member when it becomes aware of unauthorized access to sensitive member information, unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur, and takes appropriate steps to safeguard the interests of affected members, including monitoring affected members' accounts for unusual or suspicious activity. For

the purposes of the proposed Guidance, NCUA defines sensitive member information to mean a member's social security number, personal identification number (PIN), password, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. Sensitive member information would also include any combination of components of member information that would allow someone to log onto or access another person's account, such as user name and password.

Under Part 748 and Appendix A, credit unions must have a security program designed to protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member. NCUA believes that substantial harm or inconvenience is most likely to result from the improper access to and use of sensitive member information. Accordingly, the proposed Guidance anticipates that notice will be given in such cases, in order to mitigate or prevent substantial harm or inconvenience to a member.

NCUA notes that the response program described under the proposed Guidance should address incidents involving the unauthorized access to or use of any form of member information. However, the proposed Guidance anticipates that member notice will only occur in cases of security breaches involving sensitive member information.

The proposed Guidance provides several examples NCUA believes typify situations in which member notification is expected and those when it is not. As in other circumstances, NCUA also expects credit unions to notify members when directed to do so by the credit union's primary regulator.

The proposed Guidance discusses the content and delivery of member notices. The notice should include a general description of the incident, and provide information to assist members in mitigating potential harm, including a member service number, steps members can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

In addition, credit unions are expected to inform each member about the availability of the Federal Trade Commission's ("FTC") online guidance regarding measures to protect against identity theft and to encourage the member to report any suspected incidents of identity theft to the FTC. Further, credit unions should provide the FTC's Web site address and telephone number for purposes of obtaining guidance and reporting suspected incidents of identity theft. Currently, the Web site address is www.ftc.gov/idtheft, and the toll free number for the identity theft hotline is 1-877-IDTHEFT.

The proposed Guidance also describes other forms of assistance that financial institutions have offered to their customers in incidents of this type. Credit unions may wish to offer such forms of assistance to their members and describe them in the member notice.

II. Request for Comments

NCUA invites comment on all aspects of the proposed amendment of Part 748 and the proposed Guidance, including each component of the response program described in Paragraph II of the proposed Guidance. Please consider the following in formulating your comments:

- Should any component of the response program be clarified in some way and, if so, how?

- Are there additional components that should be included in a response program to address incidents involving unauthorized access to or use of member information? If so, please describe the component, and the reasons that support it.

- Should each component of the response program be retained? If not, which components should be deleted and why?

- In preparing the proposed Guidance, NCUA has attempted to identify a standard that will lead to member notice when appropriate. NCUA recognizes that there is a spectrum of alternatives for developing a requirement to notify members. On one side of the spectrum is a standard that would require a credit union to notify its members every time the mere possibility of misuse of member information arises. On the other side is a standard that would require a credit union to notify its members only when it becomes aware of an incident involving unauthorized access to member information and, based on unusual activity in members' accounts or other indicia of identity theft, knows that the information is being misused. NCUA proposes a standard that lies in the middle of this spectrum. NCUA believes that no useful purpose would be served if notices were sent due to the mere possibility of misuse of some member information. In general, the notices should alert members to those situations where enhanced vigilance is necessary to protect against fraud or identity theft. NCUA believes that notice to members is appropriate in a narrower range of instances involving the unauthorized access to sensitive member information. The proposed Guidance anticipates that a credit union would send notice to each affected member when the credit union becomes aware of an incident of unauthorized access to sensitive member information, unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including

by monitoring affected members' accounts for unusual or suspicious activity. NCUA invites comment on whether this is the appropriate standard for triggering member notice. For commenters who believe that this standard is inappropriate, NCUA requests that these commenters state specifically their reasoning and offer alternative thresholds for triggering member notice.

- The proposed Guidance defines sensitive member information as a social security number, a personal identification number (PIN), password, or an account number in conjunction with a personal identifier. Sensitive member information would also include any combination of components of member information that would allow someone to log onto or access another person's account, such as user name and password. NCUA requests comment on which, if any, additional types of information should be included in this definition, such as mother's maiden name or driver's license number.

- NCUA invites comment on the potential burden associated with the member notice provisions. For example, what is the anticipated burden that may arise from the questions posed by those members who receive the notices? Should NCUA consider how the burden may vary depending upon the size and complexity of the credit union?

- As part of the response program, NCUA describes certain corrective measures that a credit union should take once an incident of unauthorized access occurs. One such measure is to "secure accounts." Is the discussion of securing accounts sufficiently clear to enable credit unions to know what is expected of them when instances of unauthorized access occur? To what extent would contracts between credit unions and service providers need to be modified, if at all, to comply with expectations of the proposed rule and proposed Guidance? How much burden, if any, will the proposed Guidance impose on service providers?

- NCUA also invites comment on whether the proposed standard should be modified to apply to other extraordinary circumstances that compel a credit union to conclude that unauthorized access to information, other than sensitive member information, likely will result in substantial harm or inconvenience to the affected members.

- The proposed Guidance includes examples of circumstances in which member notice would be expected and those when it would not. Please comment on whether the examples in the proposed Guidance should be modified or supplemented and provide your rationale.

III. Regulatory Procedures

Paperwork Reduction Act

A. Request for Comment on Proposed Information Collection

In accordance with the requirements of the Paperwork Reduction Act of 1995, NCUA may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. NCUA has determined that the proposed rule is covered under the Paperwork Reduction Act and is submitting a copy of this proposed rule to the Office of Management and Budget (OMB) for approval as a revision of OMB control number 3133-0033, which is the control number currently associated with the collection of information under Part 748 requiring a written security program.

The proposed amendment would require federally insured credit unions to review their existing written security programs to ensure they are designed to respond to incidents of unauthorized access to or use of member information in certain circumstances. To meet this requirement, NCUA expects federally insured credit unions will: (1) develop notices to members, (2) determine which members should receive the notices and send the notices to members, and (3) ensure that their contracts with their service providers conform to the procedures they

develop. The NCUA Board estimates it will take an average of 20 hours for a credit union to comply with the incident response element. The Board also estimates that credit unions will require 24 hours per incident (three business days) to determine which members should receive the notice and notify the members. For the purposes of this analysis, it is estimated that two percent of credit unions will experience an incident of unauthorized access to member information on an annual basis, resulting in member notification.[3]

Thus, the burden associated with this collection of information may be summarized as follows:

Number of Respondents: 9,528

Estimated Time per Response:

Developing notices: 20 hrs x 9,528 = 190,560 hours

Notifying members: 24 x 210 = 5,040 hours

Estimated Total Annual Burden: 195,600 hours

However, the burden estimate does not include time for credit unions to adjust

[3] This estimate is based upon NCUA's experience and data involving banks gathered by the FDIC that indicates slightly less than one percent of those institutions experienced some form of unauthorized access to customer information during any 12 month period. However, NCUA assumes that other incidents of unauthorized access to customer or member information may have occurred but were not reported.

their contracts with service providers, if needed; nor for service providers to disclose information pursuant to the proposed Guidance.

The Paperwork Reduction Act and OMB regulations require that the public be provided an opportunity to comment on the paperwork requirements, including an agency's estimate of the burden of the paperwork requirements. The NCUA Board invites comment on: (1) whether the paperwork requirements are necessary; (2) the accuracy of NCUA's estimates on the burden of the paperwork requirements; (3) ways to enhance the quality, utility, and clarity of the paperwork requirements; and (4) ways to minimize the burden of the paperwork requirements.

Comments should be sent to: OMB Reports Management Branch, New Executive Office Building, Room 10202, Washington, DC 20503; Attention: Joseph Lackey, Desk Officer for NCUA. Please send NCUA a copy of any comments submitted to OMB.

Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. §§ 601-612) (RFA) requires an agency to publish an initial regulatory flexibility analysis whenever the agency is required to publish a general notice of proposed rulemaking for a proposed rule unless it is determined that the proposed rule will not have a significant economic impact on a substantial number of small entities. The Board cannot at this time determine whether the proposed rule would have significant economic impact on a substantial number of small entities. Therefore, pursuant to subsections 603(b) and (c) of the RFA, the Board provides the following initial regulatory flexibility analysis.

A. Reasons for Proposed Rule

The NCUA is requesting comment on a proposed amendment to Part 748 of its regulations and guidelines for credit unions in the form of Appendix B. These proposals augment existing requirements and guidance regarding the security of member records previously adopted pursuant to Section 501 of the GLBA. Section 501 requires the Agencies to publish standards for financial institutions relating to administrative, technical, and physical standards 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 which could result in substantial harm or inconvenience to any customer. The reasons for NCUA's actions are further described in the Supplementary Information section.

B. Statement of Objectives and Legal Basis

The **Supplementary Information** section above contains this information. The legal basis for the proposed rule is the GLBA.

C. Estimate of Small Credit Unions to Which the Rule Applies

The proposed rule would apply to all federally insured credit unions. Small credit unions are defined by NCUA as those with less than $10,000,000 in assets of which there are approximately 4,646. Interpretive Ruling and Policy Statement (IRPS) 87-2, Developing and Reviewing Government Regulations, 52 FR 35231 (Sep. 18, 1987), as amended by IRPS 03-2 68 FR 31949 (May 29, 2003).

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

The information collection requirements imposed by the proposed rule are discussed above in the section on the Paperwork Reduction Act.

E. General Requirements

Credit unions are already required under the GLBA and Section 748.0 of NCUA's Rules and Regulations to develop an information security program to safeguard member information. Development of such a program involves assessing risks to member information, establishing policies, procedures, and training to control risks, testing the program's effectiveness, and managing and monitoring service providers. This proposed rule would require that the information security program contain an element that is designed to respond to incidents involving breach of information integrity. The NCUA believes that the establishment of information security programs is a sound business practice for a credit union and is already addressed by existing supervisory procedures. However, the proposed rule may require some credit unions to enhance existing information security programs, but the cost of doing so is not known. The NCUA seeks any information or comment on the costs of enhancing existing information security programs.

F. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The NCUA is unable to identify any statutes or rules which would overlap or conflict with the requirement to assure that existing information security programs contain a response element relating to breaches of information integrity. The

NCUA seeks comment and information about any such statutes or rules, as well as any other state, local, or industry rules or policies that require a credit union to implement business practices that would comply with the requirements of the proposed rule.

G. Discussion of Significant Alternatives

As previously noted, credit unions are already required by GLBA and existing regulation to develop and implement a meaningful security program. The proposed rule would require that such security programs include a provision for appropriate responses to incidents involving a breach of information integrity. Consistent with the position taken by the other Agencies, the NCUA views this as a fundamental element of any information security program. However, the proposed rule also provides substantial flexibility so that any credit union, regardless of size, may adopt an information security program tailored to its individual needs. The NCUA welcomes comment on any significant alternatives, consistent with the GLBA that would minimize the impact on small credit unions.

Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on state and local interests. In adherence to fundamental federalism principles, NCUA, an independent regulatory agency as

defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. The proposed rule would not have substantial direct effects on the states, on the connection between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined that this proposed rule does not constitute a policy that has federalism implications for purposes of the executive order.

The Treasury and General Government Appropriations Act, 1999 - - Assessment of Federal Regulations and Policies on Families

The NCUA has determined that this proposed rule would not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Pub. L. 105-277, 112 Stat. 2681 (1998).

Agency Regulatory Goal

NCUA's goal is to promulgate clear and understandable regulations that impose minimal regulatory burden. We request your comments on whether the proposed rule is understandable and minimally intrusive.

List of Subjects

12 CFR Part 748

Credit unions, Crime, Currency, Reporting and recordkeeping requirements and Security measures.

By the National Credit Union Administration Board on October 23, 2003

_____
Becky Baker

Secretary of the Board

For reasons set forth in the preamble, the NCUA Board proposes to amend 12 CFR 748 as follows:

PART 748 – Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance.

1. The authority citation for Part 748 continues to read as follows:

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

2. In §748.0 revise paragraph (b) to read as follows:

§748.0 Security Program

* * * * * *

(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

(5) prevent destruction of vital records, as defined in the Accounting Manual for Federal Credit Unions.

3. Add Appendix B to read as follows:

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,[1] interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and describes NCUA's expectations regarding how federally insured credit unions should develop and implement response programs, including member notification procedures, to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

Security Guidelines

Section 501(b) of the GLBA required NCUA to establish appropriate standards for credit unions subject to its jurisdiction that include administrative, technical,

[1] 12 C.F.R. Part 748.

and physical safeguards to protect the security and confidentiality of member information.[2] Accordingly, NCUA amended Part 748 of its rules to require credit unions to develop appropriate security programs, and issued Appendix A to Part 748 (Appendix A), reflecting its expectation that every federally insured credit union would develop an information security program 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.

Risk Assessment and Controls

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

[2] The term "member information" is the same term used in Appendix A and means any record containing nonpublic personal information whether in paper, electronic, or other form, maintained by or on behalf of the credit union.

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

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

- The sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[3]

Following the assessment of these risks, Appendix A calls for 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,[4] and adopt those that are appropriate for the credit union, including:

- Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to

[3] See Appendix A, Paragraph III.B.
[4] See Appendix A, Paragraph III.C.

prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

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

- 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.[5]

Service Providers

Appendix A advises every credit union to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.[6] Consistent with existing guidance issued by the Agencies, a credit union's contract with its service provider should require the service provider to fully disclose to the credit union information relating to any breach in security resulting in an unauthorized intrusion into the credit union's

[5] See Appendix A, Paragraph III.C.1.g.
[6] See Appendix A, Paragraphs II.B. and III.D.

member information systems maintained by the service provider.[7] In view of these contractual obligations, the service provider would be required to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information to enable the credit union to expeditiously implement its response program.[8]

Response Program

As internal and external threats to the security of member information are reasonably foreseeable and may lead to the misuse of member information, NCUA expects every federally-insured credit union to develop a response program to protect against the risks associated with these threats. The response program should include measures to protect member information in member information systems maintained by the credit union or its service providers. NCUA expects that member notification will be a component of a credit union's response program, as described below.

[7] See NCUA Letter to Credit Unions No. 00-CU-11, Risk Management of Outsourced Technology Services, Dec, 2000.

[8] NCUA is aware 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 (FTC). 12 CFR part 314 applies to the handling of all customer information possessed by any financial institution subject to the jurisdiction of the FTC, regardless of whether such information pertains to individuals with whom the institution has a customer relationship or pertains to the customers of other financial institutions that have provided such information to that institution.

II. Components of a Response Program

A response program should be a key part of a credit union's information security program.[9] Having such a program in place will allow the credit union to quickly respond[10] to incidents involving the unauthorized access to or use of member information in its own member information systems that could result in substantial harm or inconvenience to a member. Under Appendix A, a credit union's *member information systems* consist 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.[11]

Timely notification of members, under the circumstances described below, is important to manage a credit union's reputation risk. Effective notice may reduce 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.

A response program should contain the following components:

[9] See FFIEC Information Security Booklet, Dec. 2002.
[10] Credit unions are expected to provide employees with the training necessary to understand their roles and responsibilities in order to expeditiously implement the credit union's response program to address incidents of unauthorized access to and use of member information.
[11] See Appendix A, Paragraph I.B.2.c

A. Assess the Situation

The credit union should assess the nature and scope of the incident, and identify what member information systems and types of member information have been accessed or misused.

B. Notify Regulatory and Law Enforcement Agencies

The credit union should promptly notify NCUA or its primary state regulator when it becomes aware of an incident involving unauthorized access to or use of member information that could result in substantial harm or inconvenience to its members.

A credit union also should file a Suspicious Activity Report ("SAR"), if required, in accordance with the applicable SAR regulations[12] and NCUA guidance.[13] Consistent with NCUA's SAR regulations, in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, the credit union should immediately notify, by telephone, appropriate law enforcement authorities and NCUA or its primary state regulator, in addition to filing a timely SAR.

[12] 12 CFR § 748.1(c)
[13] NCUA Letter to Credit Unions No. 00-CU-04, Suspicious Activity Reporting, July 2000.

C. Contain and Control the Situation

The credit union should take measures to contain and control the incident to prevent further unauthorized access to or use of member information, while preserving records and other evidence.[14] Depending upon the particular facts and circumstances of the incident, these measures could include, in connection with computer intrusions: (i) shutting down applications or third party connections; (ii) reconfiguring firewalls in cases of unauthorized electronic intrusion; (iii) ensuring that all known vulnerabilities in the credit union's computer systems have been addressed; (iv) changing computer access codes; (v) modifying physical access controls; and (vi) placing additional controls on service provider arrangements.

D. Corrective measures

Once a credit union understands the scope of the incident and has taken steps to contain and control the situation, it should take measures to address and mitigate the harm to individual members. For example, the credit union should take the following measures:

[14] See FFIEC Information Security Booklet, Dec. 2002, pp. 68-74.

1. Flag Accounts

The credit union should immediately begin identifying and monitoring the accounts of those members whose information may have been accessed or misused. In particular, the credit union should provide staff with instructions regarding the recording and reporting of any unusual activity, and if indicated given the facts of a particular incident, implement controls to prevent the unauthorized withdrawal or transfer of funds from member accounts.

2. Secure Accounts

When a share draft, savings, deposit or other account number, debit or credit card account number, personal identification number (PIN), password, or other unique identifier has been accessed or misused, the credit union should secure the account, and all other accounts and credit union services that can be accessed using the same account number or name and password combination until such time as the credit union and the member agree on a course of action.[15]

3. Member Notice and Assistance

Under Part 748 and Appendix A, a credit union's security program must be designed to protect its members' information against unauthorized access or use.

[15] The credit union should also consider the use of new account numbers and steps to ensure that members do not reuse the same or a similar personal identification number.

A credit union should not forgo notifying its members of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so. Under the circumstances described in Appendix A, the credit union should notify and offer assistance to members whose information was the subject of the incident.[16] If the credit union is able to determine from its logs or other data precisely which members' information was accessed or misused, it may restrict its notification to those individuals. However, if the credit union cannot identify precisely which members are affected, it should notify each member in groups likely to have been affected, such as each member whose information is stored in the group of files in question.

a. Delivery of Member Notice – Member notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the member is likely to receive it. For example, the credit union may choose to contact all members affected by telephone or by mail, or for those members who conduct transactions electronically, using electronic notice.

b. Content of Member Notice –The notice should describe the incident in general terms and the member's information that was the subject of unauthorized access or use. It should also include a number that members can call for further information and assistance. The notice also should remind members of the need

[16] The credit union should, therefore, ensure that a sufficient number of appropriately trained employees are available to answer member inquiries and provide assistance.

to remain vigilant, over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft.

Key Elements: In addition, the notice should:

- Inform affected members that the credit union will assist the member to correct and update information in any consumer report relating to the member, as required by the Fair Credit Reporting Act;

- Recommend that the member notify each nationwide credit reporting agency to place a fraud alert[17] in the member's consumer reports;

- Recommend that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

- Inform the member of the right to obtain a credit report free of charge, if the member has reason to believe that the file at the consumer reporting agency contains inaccurate information due to fraud, together with contact information regarding the nationwide credit reporting agencies; and

[17] A fraud alert will put the member's creditors on notice that the member may be a victim of fraud.

- Inform the member about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft, and encourage the member to report any incidents of identity theft to the FTC. The notice 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.[18]

Optional Element: Credit unions also may wish to provide members with the following additional types of assistance that have been offered under these circumstances:

- Provide a toll-free telephone number that members can call for assistance;

- Offer to assist the member in notifying the nationwide credit reporting agencies of the incident and in placing a fraud alert in the member's consumer reports; and

[18] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *www.ftc.gov/idtheft* and 1-877-IDTHEFT.

- Inform the member about subscription services that provide notification anytime there is a request for the member's credit report or offer to subscribe the member to this service, free of charge, for a period of time.

The credit union may also wish to include with the notice a brochure regarding steps a member can take to protect against identity theft, prepared by the Agencies that can be downloaded from the Internet.[19]

III. Circumstances for Member Notice

Standard for Providing Notice

A credit union should notify affected members whenever it becomes aware of unauthorized access to sensitive member information unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including by monitoring affected members' accounts for unusual or suspicious activity.

[19] *www.occ.treas.gov/idtheft.pdf; www.federalreserve.gov/consumers.htm; www.fdic.gov/consumers/consumer/news/cnsum00/idthft.html.*

Sensitive Member Information

Under Part 748 and Appendix A, a credit union must have a written security program designed to 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 easily misused, as in the commission of identity theft. For purposes of this Guidance, sensitive member information means a member's social security number, personal identification number, password or account number, in conjunction with a personal identifier such as the member's name, address, or telephone number. Sensitive member information would also include any combination of components of member information that would allow someone to log onto or access another person's account, such as user name and password. Therefore, credit unions are expected to notify affected members when sensitive member information has been improperly accessed, unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members.

Examples of When Notice Should be Given

A credit union should notify affected members when it is aware of the following incidents unless the credit union, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members.

- An employee of the credit union has obtained unauthorized access to sensitive member information maintained in either paper or electronic form;

- A cyber intruder has broken into an credit union's unencrypted database that contains sensitive member information;

- Computer equipment such as a laptop computer, floppy disk, CD-ROM, or other electronic media containing sensitive member information has been lost or stolen;

- A credit union has not properly disposed of member records containing sensitive member information; or

- The credit union's third party service provider has experienced any of the incidents described above, in connection with the credit union's sensitive member information.

Examples of When Notice is Not Expected

A credit union is not expected to give notice when it becomes aware of an incident of unauthorized access to member information, and the credit union, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members. For example, a credit union would not need to notify affected members in connection with the following incidents:

- The credit union is able to retrieve sensitive member information that has been stolen, and reasonably concludes, based upon its investigation of the incident, that it has done so before the information has been copied, misused or transferred to another person who could misuse it;

- The credit union determines that sensitive member information was improperly disposed of, but can establish that the information was not retrieved or used before it was destroyed;

- A hacker accessed files that contain only member names and addresses; or

- A laptop computer containing sensitive member information is lost, but the data is encrypted and may only be accessed with a secure token or similarly secure access device.