Appendix B to Part 748—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

I. BACKGROUND

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

[29] 12 CFR Part 748.

A. Security Guidelines

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

1. Ensure the security and confidentiality of member information;

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

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

B. Risk Assessment and Controls

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

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

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

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

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

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:

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

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]

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

C. 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. [33]

[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 ("FTC"), 12 CFR Part 314.

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.

[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.htm1#infosec,* for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

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.

[38] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, (June 2004), available at *http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.htm1#outscouring* for additional guidance on managing outsourced relationships.

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;

[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.

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

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

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:

[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.

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

[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).

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]