

(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, 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:

- 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 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 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.

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 respond¹⁰ 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:

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 regulations¹² 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

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.

¹² 12 CFR 748.1(c).

¹³ NCUA Letter to Credit Unions No. 00-CU-04, Suspicious Activity Reporting, July 2000.

¹ 12 CFR part 748.

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.

³ See appendix A, paragraph III.B.

⁴ See appendix A, paragraph III.C.

⁵ See appendix A, paragraph III.C.1.g.

⁶ See appendix A, paragraphs II.B. and III.D.

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.