7535-01-U

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

Guidelines for Safeguarding Member Information.

AGENCY: National Credit Union Administration (NCUA).

ACTION: Final Rule.

SUMMARY: The NCUA Board is modifying its security program requirements to include security of member information. Further, the NCUA Board is issuing "Guidelines for Safeguarding Member Information" to implement certain provisions of the Gramm-Leach-Bliley Act (the GLB Act or Act).

The GLB Act requires the NCUA Board to establish appropriate standards for federally-insured credit unions relating to administrative, technical, and physical safeguards for member records and information. These safeguards are intended to: insure the security and confidentiality of member records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any member.

DATES: This rule is effective July 1, 2001.

ADDRESSES: National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428.

FOR FURTHER INFORMATION CONTACT: Matthew Biliouris, Information Systems Officer, Office of Examination and Insurance, at the above address or telephone (703) 518-6360.

SUPPLEMENTARY INFORMATION:
The contents of this preamble are listed in the following outline:

I. Background

On November 12, 1999, President Clinton signed the GLB Act (Pub. L. 106-102) into law. Section 501, entitled Protection of Nonpublic Personal Information, requires the NCUA Board, the federal banking agencies (including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision), the Securities and Exchange Commission, state insurance authorities, and the Federal Trade Commission (collectively, the "Agencies") to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to the administrative, technical, and physical safeguards for customer records and information. These safeguards are intended 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 would result in substantial harm or inconvenience to any customer.

Section 505(b) of the GLB Act provides that these standards are to be implemented by the NCUA and the federal banking agencies in the same manner, to the extent practicable, as standards pursuant to section 39(a) of the Federal Deposit Insurance Act (FDIA). Section 39(a) of the FDIA requires the federal banking agencies to establish operational and managerial standards for insured depository institutions relative to, among other things, internal controls, information systems, and internal audit systems, as well as such other operational and managerial standards as determined to be appropriate. 12 U.S.C. 1831p(a). Section 39 of the FDIA provides for standards to be prescribed by guideline or by rule. 12 U.S.C. 1831p(d)(1). The FDIA also provides that if an institution fails to comply with a standard issued as a rule, the institution must submit a compliance plan within particular time frames, while if an institution fails to comply with a standard issued as a guideline, the agency has the discretion as to whether to require an institution to submit a compliance plan. 12 U.S.C. 1831p(e)(1).

Section 39 of the FDIA does not apply to the NCUA, and the Federal Credit Union Act does not contain a similar, regulatory framework for the issuance and enforcement of standards. In preparation of NCUA's regulation and appendix with guidelines, NCUA staff worked with an interagency group that included representatives from the federal banking agencies. The NCUA Board's understanding is that the federal banking agencies recently have approved standards by guidelines issued as appendices to their safety and soundness standards.

The NCUA Board has determined that it can best meet the congressional directive to prescribe standards through an amendment to NCUA's existing regulation governing security programs in federally-insured credit unions. The final regulation requires that federally-insured credit unions establish a security program addressing the safeguards required by the GLB Act. The Board is also issuing an appendix to the regulation that sets out guidelines, the text of which is substantively identical to the guidelines approved by the federal banking agencies. The guidelines are intended to outline

industry best practices and assist credit unions to develop meaningful and effective security programs to ensure their compliance with the safeguards contained in the regulation.

Currently, NCUA regulations require that federally-insured credit unions have a written security program designed to protect each credit union from robberies, burglaries, embezzlement, and assist in the identification of persons who attempt such crimes. Expanding the environment of protection to include threats or hazards to member information systems is a natural fit within a comprehensive security program. To evaluate compliance, the NCUA will expand its review of credit union security programs and annual certifications. This review will take place during safety and soundness examinations for federal credit unions and within the established oversight procedures for state-chartered, federally-insured credit unions. If a credit union fails to establish a security program meeting the regulatory objectives, the NCUA Board could take a variety of administrative actions. The Board could use its cease and desist authority, including its authority to require affirmative action to correct deficiencies in a credit union's security program. 12 U.S.C. 1786(e) and (f). In addition, the Board could employ its authority to impose civil money penalties. 12 U.S.C. 1786(k). A finding that a credit union is in violation of the requirements of §748.0(b)(2) would typically result only if a credit union fails to establish a written policy or its written policy is insufficient to reasonably address the objectives set out in the proposed regulation.

The guidelines apply to "nonpublic personal information" of "members" as those terms are defined in 12 CFR part 716, NCUA's rule captioned Privacy of Consumer Financial Information (the Privacy Rule or Part 716). See 65 FR 31722, May 18, 2000. Under section 503(b)(3) of the GLB Act and Part 716, credit unions will be required to disclose their policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information as part of the initial and annual notices to their members. Defining terms consistently should facilitate the ability of credit unions to develop their privacy notices in light of the guidelines set forth here. NCUA derived key components of the guidelines from security-related supervisory guidance developed with the federal banking agencies through the Federal Financial Institutions Examination Council (FFIEC).

The NCUA Board requested comment on all aspects of the proposed amendment of §748.0 and the guidelines, as well as comment on the specific provisions and issues highlighted in the section-by-section analysis below.

II. Overview of Comments Received

On June 6, 2000, the NCUA Board approved a proposal to revise 12 CFR part 748 to include requirements for administrative, technical, and physical safeguards for member records and information, as required by the GLB Act. 65 FR 37302, Jun. 14, 2000. The comment period for the proposed rule ended August 14, 2000. NCUA received 13 comments on the proposal: two from natural person credit unions, one from a corporate credit union, two from national credit union trade associations, seven from state credit union leagues, and one from a miscellaneous trade group. In addition, the

other FFIEC Agencies collectively received a total of 206 comments. While NCUA carefully considered all comments on our proposed rule, to remain as consistent as practicable with the other FFIEC Agencies, NCUA has made some changes in the final rule as a result of interagency discussions.

NCUA invited comment on all aspects of the proposed guidelines, including whether the rule should be issued as guidelines or as regulation. Commenters overwhelmingly supported the adoption of guidelines as discussed below. Several commenters cited the benefits of flexibility and the drawbacks of prescriptive requirements that could become rapidly outdated as a result of changes in technology.

In light of the comments received, the NCUA has decided to adopt the guidelines, with several changes as discussed below to respond to the commenters' suggestions.

In directing the Agencies to issue standards for the protection of customer records and information, Congress provided that the standards apply to all financial institutions, regardless of the extent to which they may disclose information to affiliated or nonaffiliated third parties, electronically transfer data with customers or third parties, or record data electronically. Because the requirements of the Act apply to a broad range of financial institutions, the NCUA and the other FFEIC Agencies believe that the guidelines must establish appropriate standards that allow each institution the discretion to design an information security program that suits its particular size and complexity and the nature and scope of its activities. In some instances, credit unions already will have information security programs that are consistent with these guidelines. In such situations, little or no modification to a credit union's program will be required.

Below is a section-by-section analysis of the final guidelines.

III. Section-by-Section Analysis

The discussion that follows applies to the final rule Part 748.

The security program in §748.0(b) previously addressed only those threats due to acts such as robberies, burglaries, larcenies, and embezzlement. In the emerging electronic marketplace, the threats to members, credit unions, and the information they share to have a productive, technologically competitive, financial relationship have increased. The security programs to ensure protections against these emerging crimes and harmful actions must keep pace. Congress directed in section 501(b) of the GLB Act that the Agencies establish standards to ensure financial institutions protect the security and confidentiality of the nonpublic personal information of their customers.

To meet this directive, the proposed rule revised paragraph (b) of §748.0 to require that a credit union's security program include protections to ensure the security and confidentiality of member records, protect against 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 inconvenience to a member. This modification expanded the security program objectives to include the emerging

threats and hazards to members, credit unions, and the information they share to have a financial relationship.

NCUA has adopted this revision as proposed with one exception. NCUA has changed the reference in section 748.0(b)(4) from "the Accounting Manual for Federal Credit Unions", to "12 CFR part 749." NCUA is currently revising Part 749 regarding a credit union's preservation of vital records.

The discussion that follows applies to the NCUA's final guidelines.

APPENDIX A TO PART 748 – GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

I. Introduction

Paragraph I. sets forth the general purpose of the guidelines, which is to provide guidance to each credit union in establishing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information. This paragraph also sets forth the statutory authority for the final guidelines, sections 501 and 505(b) of the GLB Act. 15 U.S.C. 6801 and 6805(b). The NCUA received no comments on this paragraph, and has adopted it as proposed.

I.A. Scope

Paragraph I.A. describes the scope of the proposed guidelines. The guidelines apply to member information maintained by or on behalf of all federally-insured credit unions. NCUA has adopted the scope as proposed.

The NCUA received a comment requesting clarification on whether the rule includes corporate credit unions. This commenter indicated that because of the use of the word "consumer" throughout the proposed rule, it is feasible to presume that the proposed rule is referring only to natural person credit unions.

The general purpose of the guidelines is to provide guidance to credit unions in establishing and implementing safeguards to protect member information. It appears that a corporate credit union will rarely have natural person members or customers. Such members appear to be limited to those corporate credit unions that have natural person incorporators that maintain a share account. Those members are limited in number. However, if a corporate credit union has a natural person member, it will be required to establish and implement safeguards to protect the member's information.

This commenter requested clarification on whether the proposed rule pertains to corporate credit unions as a "service provider," or as a credit union that must comply with the regulation. The commenter also asked whether there is an exemption for corporate credit unions providing service to natural person credit unions that is part of normal processing business. Natural person credit unions that use corporate credit unions as their "service providers" will likely look to the guidelines in overseeing their

service provider arrangements with those corporate credit unions. There is no exemption for corporate credit unions that provide services to natural person credit unions as part of normal processing business. NCUA notes that disclosure pursuant to one of the exceptions in the Privacy Rule does not constitute unauthorized access under the guidelines. (See II.B. Objectives.).

I.B. Definitions

Paragraph I.B. sets forth the definitions of various terms for purposes of the guidelines. The defined terms have been placed in alphabetical order in the final guidelines.

I.B.1. In general

Paragraph I.B.1. provides that terms used in the guidelines have the same meanings as set forth in 12 CFR part 716, except to the extent that the definition of a term is modified in the guidelines or where the context requires otherwise.

The NCUA and other FFIEC Agencies received several comments on the proposed definitions. NCUA has made certain changes in its final rule as discussed below.

Member (I.B.2.a.)

Proposed paragraph I.B.3. defined "member" in the same way as that term is defined in section 716.3(n) of the Privacy Rule. The NCUA proposed to use this definition in the guidelines because section 501(b) refers to safeguarding the security and confidentiality of member information. Given that Congress used the same term for both the 501(b) standards and for the sections concerning financial privacy, NCUA has concluded that it is appropriate to use the same definition in the guidelines that was adopted in the Privacy Rule.

The term "member" includes individuals who are not actually members, but are entitled to the same privacy protections under Part 716 as members. Examples of individuals that fall within the definition of member in Part 716 are nonmember joint account holders, nonmembers establishing an account at a low-income designated credit union, and nonmembers holding an account in a state-chartered credit union under state law. The term "member" does not cover business members or consumers who have not established an ongoing relationship with the credit union (e.g., those consumers that merely use an ATM or purchase travelers checks). See 12 CFR 716.3(n) and (o).

The NCUA Board solicited comment on whether the definition of member should be broadened to provide a common information security program for all types of records under the control of a credit union. The NCUA received many comments on this definition, almost all of which agreed with the proposed definition. Although a few commenters indicated they would apply the same security program to both business and consumer records, the vast majority of commenters supported the use of the same definition of member in the guidelines as is used in the Privacy Rule. They observed that the use of the term customer in section 501 of the GLB Act, when read in the

context of the definitions of consumer and customer relationship in section 509, reflects the Congressional intent to distinguish between certain kinds of consumers for the information security standards and the other privacy provisions established under subtitle A of Title V.

The NCUA believes, therefore, that the most reasonable interpretation of the applicable provisions of subtitle A of Title V of the Act is that a credit union is obligated to protect the security and confidentiality of the nonpublic personal information of its consumers with whom it has a member relationship. As a practical manner, a credit union may also design or implement its information security program in a manner that encompasses the records and information of its other consumers and its business clients.[1]

Member information (I.B.2.b.)

Section 501(b) refers to safeguarding the security and confidentiality of "customer information." The term "customer" is also used in other sections of Title V of the GLB Act. As stated above, the NCUA Board used the term "member" in place of the term "customer" in implementing these sections of the GLB Act in Part 716.

Proposed paragraph I.B.2. defined member information as any records containing nonpublic personal information, as defined in section 716.3(q) of the Privacy Rule, about a member. This included records, data, files, or other information in paper, electronic, or other form that are maintained by any service provider on behalf of the institution. Although section 501(b) of the GLB Act refers to the protection of both customer records and information, for the sake of simplicity, the proposed guidelines used the term "member information" to encompass both information and records.

The NCUA did not receive any comments specifically relating to this definition. The NCUA has adopted a definition of "member information" that is substantially the same as the proposed definition. The NCUA has, however, deleted the reference to data, files, or other information from the final guidelines, since each is included in the term "records" and also is covered by the reference to "paper, electronic, or other form."

[1] The NCUA and the other FFIEC Agencies recognize that customer is defined more broadly under Subtitle B of Title V of the Act, which, in general, makes it unlawful for any person to obtain or attempt to obtain customer information of a financial institution by making false, fictitious, or fraudulent statements. For the purposes of that subtitle, the term customer means any person (or authorized representative of a person) to whom the financial institution provides a product or service, including that of acting as a fiduciary. (See section 527(1) of the Act.) In light of the statutory mandate to prescribe such revisions to such regulations and guidelines as may be necessary to ensure that such financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information (section 525), the NCUA considered modifying these guidelines to cover other customers, namely, business entities and individuals who obtain financial products and services for purposes other than personal, family, or household purposes. The NCUA has concluded, however, that defining member to accommodate the range of objectives set forth in Title V of the Act is unnecessary. Instead, the NCUA has included a new paragraph III.C.1.i, described below, and plan to issue guidance and other revisions to the applicable regulations, as may be necessary, to satisfy the requirements of section 525 of the Act.

Member information system (I.B.2.c.)

Proposed paragraph I.B.5. defined "member information system" to be electronic or physical methods used to access, collect, store, use, transmit, or protect member information. The NCUA did not receive any comments specifically relating to this definition.

The NCUA has adopted the definition of member information system largely as proposed. However, the phrase "electronic or physical" in the proposal has been deleted because each is included in the term "any method." The NCUA also has added a specific reference to records disposal in the definition of "member information system." This is consistent with the proposal's inclusion of access controls in the list of items a credit union is to consider when establishing security policies and procedures (see discussion of paragraph III.C.1.a., below), given that inadequate disposal of records may result in identity theft or other misuse of member information. Under the final guidelines, a credit union's responsibility to safeguard member information continues through the disposal process.

Service provider (I.B.2.d.)

The proposal defined a "service provider" as any person or entity that maintains or processes member information for a credit union, or is otherwise granted access to member information through its provision of services to a credit union. One commenter, a corporate credit union, asked for clarification with regard to "service provider."

The NCUA believes that the Act requires each credit union to adopt a comprehensive information security program that is designed to protect against unauthorized access to or use of members' nonpublic personal information. Disclosing information to a person or entity that provides services to a credit union creates additional risks to the security and confidentiality of the information disclosed. In order to protect against these risks, a credit union must take appropriate steps to protect information that it provides to a service provider, regardless of who the service provider is or how the service provider obtains access. The fact that an entity obtains access to member information through, for instance, providing professional services does not obviate the need for the credit union to take appropriate steps to protect the information. Accordingly, the NCUA has determined that, in general, the term "service provider" should be broadly defined to encompass a variety of individuals or companies that provide services to the credit union.

This does not mean, however, that a credit union's methods for overseeing its service provider arrangements will be the same for every provider. As explained in the discussion of paragraph III.D., below, a credit union's oversight responsibilities will be shaped by the credit union's analysis of the risks posed by a given service provider. If a service provider is subject to a code of conduct that imposes a duty to protect member information consistent with the objectives of these guidelines, a credit union may take that duty into account when deciding what level of oversight it should provide.

Moreover, a credit union will be responsible under the final guidelines for overseeing its service provider arrangements only when the service is provided directly to the credit union. The NCUA clarified this point by amending the definition of "service provider" in the final guidelines to state that it applies only to a person or entity that maintains, processes, or otherwise is permitted access to member information through its provision of services directly to the credit union.

In situations where a service provider hires a subservicer[2], the subservicer would not be a service provider under the final guidelines. The NCUA recognize that it would be inappropriate to impose obligations on a credit union to select and monitor subservicers in situations where the credit union has no contractual relationship with that person or entity. When conducting due diligence in selecting its service providers (see discussion of paragraph III.D., below), however, a credit union must determine that the service provider has adequate controls to ensure that the subservicer will protect the member information in a way that meets the objectives of these guidelines.

II. Standards for Safeguarding Member Information

II.A. Information Security Program

The proposed guidelines described NCUA's expectations for the creation, implementation, and maintenance of an information security program. As noted in the proposal, this program must include administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities.

Several interagency commenters representing large organizations were concerned that the term "comprehensive information security program" required a single uniform document that must apply to all component parts of the organization. In response, the NCUA and the other FFIEC Agencies note that a program that includes administrative, technical, and physical safeguards will, in many instances, be composed of more than one document. Moreover, use of this term does not require that all parts of an organization implement a uniform program. However, the NCUA will expect a credit union to coordinate all the elements of its information security program. Where the elements of the program are dispersed throughout the credit union, management should be aware of these elements and their locations. If they are not maintained on a consolidated basis, management should have an ability to retrieve the current documents from those responsible for the overall coordination and ongoing evaluation of the program.

II.B. Objectives

Proposed paragraph II.B. described the objectives that each credit union's information

[2] The term subservicer means any person who has access to an credit union's member information through its provision of services to the service provider and is not limited to mortgage subservicers.

security program should be designed to achieve. These objectives tracked the objectives as stated in section 501(b)(1)-(3), adding only that the security program is to protect against unauthorized access that could risk the safety and soundness of the credit union. NCUA's proposed rule also noted that unauthorized access to or use of member information does not include access to or use of member information with the member's consent.

The NCUA Board requested comment on whether there are additional or alternative objectives that should be included in the guidelines. The NCUA received several comments on this proposed paragraph, most of which indicated that the guidelines should not include any additional or alternative objectives.

First, NCUA and the other FFIEC Agencies made two changes to this objective in the final rule. NCUA notes that it does not believe the statute mandates a standard of absolute liability for a credit union that experiences a security breach. Thus, the NCUA and other FFEIC Agencies have clarified these objectives in the final rule by stating that each security program is to be designed to accomplish the objectives stated.

Second, in response to comments that objected to the addition of the safety and soundness standard, the NCUA and other FFIEC Agencies have deleted that reference in order to make the statement of objectives identical to the objectives identified in the statute. NCUA believes that risks to the safety and soundness of a credit union may be addressed through other supervisory or regulatory means, making it unnecessary to expand the statement of objectives in this rulemaking.

NCUA notes that for purposes of the guidelines, access to or use of member information is permitted if it is done with the member's consent. When a member gives consent to a third party to access or use that member's information, such as by providing the third party with an account number, PIN, or password, the guidelines do not require the credit union to know about the arrangement or to monitor the use or redisclosure of the member's information by the third party. Finally, unauthorized access does not mean disclosure pursuant to one of the exceptions in the Privacy Rule.

III. Development and Implementation of Information Security Program

III.A. Involve the Board of Directors

Proposed paragraph III.A. described the involvement of the board of directors and management in the development and implementation of an information security program. As explained in the proposal, the board of director's responsibilities are to: (1) approve the credit union's written information security policy and program; and (2) oversee efforts to develop, implement, and maintain an effective information security program, including reviewing reports from management. The proposal also outlined management's responsibilities for developing, implementing, and maintaining the security program. The NCUA did not receive any comments specifically relating to the requirement of board approval of the information security program.

NCUA believes that a credit union's overall information security program is critical to the safety and soundness of the credit union. Therefore, the final guidelines continue to place responsibility on a credit union's board of directors to approve and exercise general oversight over the program. However, the guidelines allow the entire board of directors of a credit union, or an appropriate committee of the board of directors to approve the credit union's written security program. In addition, the guidelines permit the board of directors to assign specific implementation responsibilities to a committee or an individual.

In those cases where a committee is established, NCUA considered requiring that the committee contain at least one member of the credit union's board of directors. Conversely, the NCUA also evaluated the impact of not allowing a member of the board of directors to serve on the committee. In both scenarios, NCUA determined the most logical approach is to allow each credit union board to determine the makeup of such a committee if established. To mandate additional requirements on the board of directors may place undue burden on small credit unions with a limited number of resources.

The NCUA received comments suggesting that use of the term "oversee" conveyed the notion that a board of directors is expected to be involved in day-to-day monitoring of the development, implementation, and maintenance of an information security program. The term "oversee" is meant to convey a board of director's conventional supervisory responsibilities. Day-to-day monitoring of any aspect of an information security program is a management responsibility. The final guidelines reflect this by providing that the board of directors must oversee the credit union's information security program, but may assign specific responsibility for its implementation.

The NCUA invited comment on whether the guidelines should require that the board of directors designate an Information Security Officer or other responsible individual who would have the authority, subject to the board's approval, to develop and administer the credit union's information security program. The NCUA received a few comments suggesting that the NCUA should not require the creation of a new position for this purpose. Only one commenter supported designating an Information Security Officer. Some commenters also stated that hiring one or more additional staff for this purpose would impose a significant burden.

NCUA believes that a credit union will not need to create a new position with a specific title for this purpose, as long as the credit union has adequate staff in light of the risks that credit union faces to its member information. Regardless of whether new staff are added, the lines of authority for development, implementation, and administration of a credit union's information security program need to be well-defined and clearly articulated.

The proposed guidelines set forth three responsibilities for management as part of its implementation of the credit union's information security program. They were to: (1) evaluate the impact on a credit union's security program of changing business arrangements and changes to member information systems; (2) document compliance with these guidelines; and (3) keep the board of directors informed of the current status

of the credit union's information security program. In response to this proposal, some commenters stated that the NCUA should allow a credit union to decide who within the institution is to carry out the tasks.

The NCUA believes that a credit union's board of directors is in the best position to determine who should be assigned specific roles in implementing the credit union's security program. Accordingly, the NCUA has deleted the separate provision assigning specific roles to management. The responsibilities that were contained in this provision are now included in other paragraphs of the guidelines.

III.B. Assess Risk

Proposed paragraph III.B. described the risk assessment process that should be used in the development of the information security program. Under the proposal, a credit union was to identify and assess the risks to member information. As part of that assessment, the credit union was to determine the sensitivity of the information and the threats to the credit union's systems. A credit union also was to assess the sufficiency of its policies, procedures, systems, and other arrangements in place to control risk. Finally, a credit union was to monitor, evaluate, and adjust its risk assessment in light of changes in areas identified in the proposal.

The NCUA did not receive any comments specifically relating this section of the proposed rule. However, the other FFIEC Agencies received several comments on these provisions. Accordingly, NCUA has amended its final rule to remain as consistent as practicable with the other Agencies.

Discussions with the other FFIEC Agencies focused on the issue of requiring credit unions to perform a sensitivity analysis as part of their risk assessment. NCUA is aware that "member information" is defined to mean "nonpublic personal information" as defined in the GLB Act, and that the GLB Act provides the same level of coverage for all nonpublic personal information.

While the NCUA agrees that all member information requires protection, the NCUA believes that requiring all credit unions to afford the same degree of protection to all member information may be unnecessarily burdensome in many cases. Accordingly, the final guidelines continue to state that credit unions should take into consideration the sensitivity of member information. Disclosure of certain information (such as account numbers or access codes) might be particularly harmful to members if the disclosure is not authorized. Individuals who try to breach the credit union's security systems may be likely to target this type of information. When such information is housed on systems that are accessible through public telecommunications networks, it may require more and different protections, such as encryption, than if it were located in a locked file drawer. To provide flexibility to respond to these different security needs in the way most appropriate, the guidelines confer upon credit unions the discretion to determine the levels of protection necessary for different categories of information. Credit unions may treat all member information the same, provided that the level of protection is adequate for all the information.

In addition, the NCUA and the other FFEIC Agencies believe that the security program should be focused on reasonably foreseeable risks. Therefore, NCUA has amended its final guidelines accordingly.

NCUA has made several other changes to this paragraph in the final rule to improve the order of the guidelines and to eliminate provisions that were redundant in light of responsibilities outlined elsewhere. For instance, while the proposal stated that the risk assessment function included the need to monitor for relevant changes to technology, sensitivity of member information, and threats to information security and make adjustments as needed, that function has been incorporated into the discussion of managing and controlling risk in paragraphs III.C.3. and III.E.

Thus, under the final guidelines as adopted, a credit union should identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems. Next, the risk assessment should consider the potential damage that a compromise of member information from an identified threat would have on the member information, taking into consideration the sensitivity of the information to be protected in assessing the potential damage. Finally, a credit union should conduct an assessment of the sufficiency of existing policies, procedures, member information systems, and other arrangements intended to control the risks it has identified.

(III.C.) Manage and Control Risk

Proposed paragraph III.C. described the steps a credit union should take to manage and the control risks identified in paragraph III.B.

Establish policies and procedures. Paragraph III.C.1 of the proposal described the elements of a comprehensive risk management plan designed to control identified risks and to achieve the overall objective of ensuring the security and confidentiality of member information. It identified 11 factors a credit union should consider in evaluating the adequacy of its policies and procedures to effectively manage these risks.

The NCUA did not receive any comments specifically relating to this section. However, based on interagency discussions, the NCUA has amended the final guidelines to state that each credit union must consider whether the security elements discussed in paragraphs III.C.1.a.-h. are appropriate for the credit union and, if so, adopt those elements a credit union concludes are appropriate. The NCUA believes that the security measures listed in III.C.I may be adapted by credit unions of varying sizes, scope of operations, and risk management structures. Consistent with that approach, the manner of implementing a particular element may vary from credit union to credit union. For example, while a credit union that offers Internet-based transaction accounts may conclude that encryption is appropriate, a different credit union that processes all data internally and does not have a transactional web site may consider other kinds of access restrictions that are adequate to maintain the confidentiality of member information.

The NCUA Board invited comment on the degree of detail that should be included in the guidelines regarding the risk management program, including which elements should be specified in the guidelines, and any other components of a risk management program that should be listed. Generally, the comments supported the level of detail conveyed in the proposed guidelines. The NCUA has adopted the provision regarding management and control of risks with the changes discussed below. Comments addressing proposed security measures that have been adopted without change also are discussed below.

Access rights. The NCUA did not receive any comments specifically addressing this area. However, because the other FFIEC Agencies received a number of comments suggesting that the reference to "access rights to customer information" in paragraph III.C.1.a. of their proposal could be interpreted to mean providing customers with a right of access to financial information. NCUA notes that the reference was intended to refer to limitations on employee access to member financial information, not to member access to information. However, this element has been deleted since limitations on employee access are covered adequately in other parts of paragraph III.C.1. (See discussion of "access controls" in paragraph III.C.1.a. of the final guidelines.)

Access controls. Paragraph III.C.1.b. of the proposed rule required a credit union to consider appropriate access controls when establishing its information security policies and procedures. These controls were intended to address unauthorized access to a credit union's member information by anyone, whether or not employed by the credit union.

The NCUA believes that this element sufficiently addresses the concept of unauthorized access, regardless of who is attempting to obtain access. This would cover, for instance, attempts through pretext calling to gather information about a credit union's members.[3] The NCUA has amended the final rule to refer specifically to pretext calling in new III.C.1.a. The NCUA does not intend for the final guidelines to require a credit union to provide its members with access to information the credit union has gathered. Instead, the provision in the final guidelines addressing access is limited solely to the issue of preventing unauthorized access to member information.

In accord with the other FFIEC agencies, the NCUA has deleted the reference in the proposed paragraph III.C.1.b. to providing access to authorized companies. The final guidelines require a credit union to consider the need for access controls in light of the credit union's various member information systems and adopt such controls as appropriate.

Dual control procedures. Paragraph III.C.1.f. of the proposed rule stated that credit unions should consider dual control procedures, segregation of duties, and employee background checks for employees with responsibility for, or access to, member

[3] Pretext calling is a fraudulent means of obtaining an individual's personal information by posing as that individual.

information. Most of the interagency comments on this paragraph focused on "dual control procedures", which refers to a security technique that uses two or more persons operating together to protect sensitive information. Both persons are equally responsible for protecting the information and neither can access the information alone.

The NCUA recognizes that dual-control procedures are not necessary for all activities, but might be appropriate for higher-risk activities. Given that the guidelines state only that a credit union should consider dual control procedures and adopt only if appropriate for that credit union, the NCUA has retained a reference to dual control procedures in the items to be considered (paragraph III.C.I.e.).

Oversight of servicers. Paragraph III.C.1.g. of the proposal was deleted. Instead, the final guidelines consolidate the provisions related to service providers in paragraph III.D.

Physical hazards and technical failures. The paragraphs of the proposed guidelines addressing protection against destruction due to physical hazards and technological failures (paragraphs III.C.1.j. and k., respectively, of the proposal) have been consolidated in paragraph III.C.1.h. of the final guidelines. The NCUA believes that this change improves clarity and recognizes that disaster recovery from environmental and technological failures often involve the same considerations.

Training. Paragraph III.C.2. of the proposed guidelines provided that a credit union's information security program should include a training component designed to train employees to recognize, respond to, and report unauthorized attempts to obtain member information. NCUA did not receive any comments specific to this section. However, for purposes of these guidelines, the NCUA believes that, as part of a training program, staff should be made aware both of federal reporting requirements and a credit union's procedures for reporting suspicious activities, including attempts to obtain access to member information without proper authority.

Therefore, the final guidelines amend the provision governing training to state that a credit union's information security program should include a training component designed to implement the credit union's information security policies and procedures. The NCUA believes that the appropriate focus for the training should be on compliance with the credit union's security program generally and not just on the limited aspects identified in proposed III.C.2. The provisions governing reporting have been moved to paragraph III.C.1.g., which addresses response programs in general.

Testing. Paragraph III.C.3. of the proposed guidelines provided that an information security program should include regular testing of key controls, systems, and procedures. The proposal provided that the frequency and nature of the testing should be determined by the risk assessment and adjusted as necessary to reflect changes in both internal and external conditions. The proposal also provided that the tests are to be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security program. Finally, the proposal stated that test results are to be reviewed by independent third parties or staff independent of

those that conducted the test. The NCUA Board requested comment on whether specific types of security tests, such as penetration tests or intrusion detections tests, should be required.

The most frequent comment regarding testing of key controls was that the NCUA should not require specific tests. Commenters noted that because technology changes rapidly, the tests specified in the guidelines will become obsolete and other tests will become the standard. Consequently, according to these commenters, the guidelines should identify areas where testing may be appropriate without requiring a credit union to implement a specific test or testing procedure. Several commenters noted that periodic testing of information security controls is a sound idea and is an appropriate standard for inclusion in these guidelines.

The NCUA believes that a variety of tests may be used to ensure the controls, systems, and procedures of the information security program work properly and also recognize that such tests will progressively change over time. The NCUA believes that the particular tests that may be applied should be left to the discretion of management rather than specified in advance in these guidelines. Accordingly, the final guidelines do not require a credit union to apply specific tests to evaluate the key control systems of its information security program.

The NCUA Board also invited comment regarding the appropriate degree of independence that should be specified in the guidelines in connection with the testing of information security systems and the review of test results. The proposal asked whether the tests or reviews of tests be conducted by persons who are not employees of the credit union. The proposal also asked whether employees may conduct the testing or may review test results, and what measures, if any, are appropriate to assure their independence.

Some commenters interpreted the proposal as almost requiring three separate teams of people to provide sufficient independence to control testing: one team to operate the system; a second team to test the system; and a third team to review test results. This approach, they argued, would be too burdensome and expensive to implement. The NCUA believes that the critical need for independence is between those who operate the systems and those who either test them or review the test results. Therefore, the final guidelines now require that tests should be conducted or reviewed by persons who are independent of those who operate the systems, including the management of those systems.

Whether a credit union should use third parties to either conduct tests or review their results depends upon a number of factors. Some credit unions may have the capability to thoroughly test certain systems in-house and review the test results but will need the assistance of third party testers to assess other systems. For example, a credit union's internal audit department may be sufficiently trained and independent for the purposes of testing certain key controls and providing test results to decision makers independent of system managers. Some testing may be conducted by third parties in connection with the actual installation or modification of a particular program. In each instance,

management needs to weigh the benefits of testing and test reviews by third parties against its own resources in this area, both in terms of expense and reliability.

Ongoing adjustment of program. Paragraph III.C.4. of the proposal required a credit union to monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its member information, and internal or external threats to information security. This provision was previously located in the paragraph titled "Manage and Control Risk." While there were no comments on this provision, the NCUA clarifies that this provision is applicable to a credit union's entire information security program. Therefore, this provision is now separately identified as new paragraph III.E. of the final guidelines, discussed below.

III.D. Oversee Service Provider Arrangements

NCUA's proposal addressed service providers in two provisions. The NCUA provided that a credit union should consider contract provisions and oversight mechanisms to protect the security of member information maintained or processed by service providers as one of the elements to be considered in establishing risk management policies and procedures (proposed paragraph III.C.1.g.). Additionally, proposed paragraph III.D. provided that, when a credit union uses an outsourcing arrangement, the credit union would continue to be responsible for safeguarding member information that it gives to the service provider. That proposed paragraph also provided that the credit union must use due diligence in managing and monitoring the outsourcing arrangement to confirm that its service providers would protect member information consistent with these guidelines.

The NCUA Board requested comment on the appropriate treatment of outsourcing arrangements, such as, whether industry best practices are available regarding effective monitoring of service provider security precautions, whether service providers accommodate requests for specific contract provisions regarding information security, and, to the extent that service providers do not accommodate these requests, whether credit unions implement effective security programs. The NCUA Board also requested comment on whether credit unions would find it helpful if the guidelines contained specific contract provisions requiring service provider performance standards in connection with the security of member information.

NCUA did not receive any comments relating to examples of best practices. However, given the varying complexity and level of services offered by credit unions, there could be a variety of best industry practices. The NCUA and other FFIEC Agencies recognize that information security practices are likely to evolve rapidly, and thus believe that it is inappropriate to include best practices in the final guidelines.

The majority of commenters opposed the NCUA providing specific contract provisions in the guidelines. One commenter cautioned the NCUA in crossing the boundary between regulator and manager in this area. Commenters also indicated that requiring specific contract provisions would not be consistent with the development of flexible guidelines and recommended against the inclusion of specific provisions.

The NCUA believes that credit unions should enter into appropriate contracts, but also believe that these contracts, alone, are inadequate. Therefore, the final guidelines, in paragraph III.D., include provisions relating to selecting, contracting with, and monitoring service providers.

The final guidelines require that a credit union exercise appropriate due diligence in the selection of service providers. Due diligence should include a review of the measures taken by a service provider to protect member information. As previously noted in the discussion of "service provider," it also should include a review of the controls the service provider has in place to ensure that any subservicer used by the service provider will be able to meet the objectives of these guidelines.

The final guidelines also require that a credit union have a contract with each of its service providers that requires each provider to implement appropriate measures designed to meet the objectives of these guidelines (as stated in paragraph II.B.). This provision does not require a service provider to have a security program in place that complies with each paragraph of these guidelines. Instead, by stating that a service provider's security measures need only achieve the objectives of these guidelines, the guidelines provide flexibility for a service provider's information security measures to differ from the program that a credit union implements. The NCUA has provided a two-year transition period during which credit unions may bring their outsourcing contracts into compliance. (See discussion of paragraph III.F.) NCUA has not included model contract language, because of the belief that the precise terms of service contracts are best left to the parties involved.

Each credit union must also exercise an appropriate level of oversight over each of its service providers to confirm that the service provider is implementing the provider's security measures. The NCUA has amended the guidelines as proposed to include greater flexibility with regard to the monitoring of service providers. A credit union need only monitor its outsourcing arrangements if such oversight is indicated by a credit union's own risk assessment. NCUA recognizes that not all outsourcing arrangements will need to be monitored in the same fashion. Some service providers will be financial institutions that are directly subject to these guidelines or other standards promulgated by their primary regulator under section 501(b). Other service providers may already be subject to legal and professional standards that require them to safeguard the credit union's member information. Therefore, the final guidelines permit a credit union to do a risk assessment taking these factors into account and determine for themselves which service providers will need to be monitored.

Even where monitoring is warranted, the guidelines do not require on-site inspections. Instead, the guidelines state that this monitoring can be accomplished, for example, through the periodic review of the service provider's associated audits, summaries of test results, or equivalent measures of the service provider. NCUA expects that credit unions will arrange, when appropriate, through contracts or otherwise, to receive copies of audits and test result information sufficient to assure the credit union that the service provider implements information security measures that are consistent with its contract

provisions regarding the security of member information. The American Institute of Certified Public Accountants Statement of Auditing Standards No. 70, captioned "Reports on the Processing of Transactions by Service Organizations" (SAS 70 report), is one commonly used external audit tool for service providers. Information contained in an SAS 70 report may enable a credit union to assess whether its service provider has information security measures that are consistent with representations made to the credit union during the service provider selection process.

III.E. Adjust the Program

Paragraphs III.B.3 and III.C.4. of the proposed rule both addressed a credit union's obligations when circumstances change. Both paragraph III.B.3. (which set forth management's responsibilities with respect to its risk assessment) and paragraph III.C.4. (which focused on the adequacy of a credit union's information security program) identified the possible need for changes to a credit union's program in light of relevant changes to technology, the sensitivity of member information, and internal or external threats to information security.

NCUA received no comments objecting to these paragraphs' statement of the need to adjust a credit union's program as circumstances change. While the NCUA Board has not changed the substance of these provisions in the final guidelines, it has, however, made a stylistic change to simplify the guidelines. The final guidelines combine, in paragraph III.E., the provisions previously stated separately. Consistent with the proposal, this paragraph provides that each credit union must monitor, evaluate, and adjust its information security program in light of 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. This would include an analysis of risks to member information posed by new technology (and any needed program adjustments) before a credit union adopts the technology in order to determine whether a security program remains adequate in light of the new risks presented.

III.F. Report to the Board

Paragraph III.A.2.c. of the proposal set out management's responsibilities for reporting to its board of directors. As previously discussed, the final guidelines have removed specific requirements for management, but instead allow a credit union to determine who within the organization should carry out a given responsibility. The board of directors reporting requirement thus has been amended to require that a credit union report to its board of directors, and that this report be at least annually. Paragraph III.F. of the final guidelines sets out this requirement.

The NCUA Board invited comment regarding the appropriate frequency of reports to the board of directors, including whether reports should be monthly, quarterly, or annually. The NCUA and the other FFIEC Agencies received a number of comments recommending that no specific frequency be mandated by the guidelines and that each financial institution be permitted to establish its own reporting period. Several commenters stated that if a reporting period is required, then it should be not less than

annually unless some material event triggers the need for an interim report.

The NCUA expects that in all cases, management will provide its board of directors (or the appropriate board committee) a written report on the information security program consistent with the guidelines at least annually. Management of credit unions with more complex information systems may find it necessary to provide information to the board of directors (or a committee) on a more frequent basis. Similarly, more frequent reporting will be appropriate whenever a material event affecting the system occurs or a material modification is made to the system. NCUA expects the content of these reports will vary for each credit union, depending on the nature and scope of its activities as well as the different circumstances that it will confront as it implements and maintains the program.

III.G. Implement the Standards

NCUA has added paragraph III.G. to the final rule to describe the timing requirements for implementing these standards. Each credit union should take appropriate steps to fully implement an information security program pursuant to these guidelines by July 1, 2001. This date is consistent with the Privacy Rule and the other FFIEC Agencies.

The NCUA believes that the dates for full compliance with these guidelines and the Privacy Rule should coincide. Credit unions are required, as part of their privacy notices, to disclose their policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. See 12 CFR 716.6(a)(8). NCUA has provided in the Appendix to its Privacy Rule that a credit union may satisfy this disclosure requirement by advising its members that the credit union maintains physical, electronic, and procedural safeguards that comply with federal standards to guard members' nonpublic personal information. See Appendix A-7. The NCUA believes that this disclosure will be meaningful only if the final guidelines are effective when the disclosure is made. If the effective date of these guidelines is extended beyond July 1, 2001, then a credit union may be placed in the position of providing an initial notice regarding confidentiality and security and thereafter amending the privacy policy to accurately refer to the federal standards once they became effective. For these reasons, the NCUA and other FFIEC Agencies have retained July 1, 2001, as the effective date for the guidelines.

However, the NCUA and the other FFIEC Agencies have included a transition rule for contracts with service providers. The transition rule, which parallels a similar provision in the Privacy Rule, provides a two-year period for grandfathering existing contracts. Thus a contract entered into on or before the date that is 30 days after publication of the final guidelines in the Federal Register satisfies the provisions of this part until July 1, 2003, even if the contract does not include provisions delineating the servicer's duties and responsibilities to protect member information described in paragraph III.D.

NCUA intends to maintain its 90-day compliance period for newly-chartered or insured credit unions found in §748.0(a). This section requires that each credit union establish its written security program within 90 days from the date of insurance. While the GLB

Act and the other FFIEC Agencies' regulations are silent as to compliance for newly chartered or insured institutions, NCUA believes it is reasonable to continue to provide this compliance time frame for such credit unions.

IV. Regulatory Procedures

A. Paperwork Reduction Act

The NCUA Board has submitted the reporting requirements in this final rule to the Office of Management and Budget (OMB) and is awaiting approval and revised issuance of OMB control number 3133-0053.

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 invited comment on: (1) whether the paperwork requirements are necessary; (2) the accuracy of NCUA's estimate 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.

Only two commenters provided feedback on this issue. One indicated the 40-hour estimate may be too burdensome for smaller credit unions and NCUA should consider minimum standards for smaller credit unions based on their sophistication, resources, and complexity. The other commenter stated that the 40-hour estimate was too low and suggested it be twice as long.

The NCUA believes these guidelines do represent minimum standards for protecting member information and are consistent with current practices among most credit unions. NCUA believes the changes made to the final rule enhance its flexibility for small credit unions, based on their own risk assessment and complexity of services. While NCUA recognizes that it may take some credit unions longer than 40 hours, the estimate is based on the average number of hours. Therefore, NCUA is retaining the 40-hour estimate.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. 601-612) requires, subject to certain exceptions, that NCUA prepare an initial regulatory flexibility analysis (IRFA) with a proposed rule and a final regulatory flexibility analysis (FRFA) with a final rule, unless NCUA certifies that the rule will not have a significant economic impact on a substantial number of small credit unions. For purposes of the Regulatory Flexibility Act, and in accordance with NCUA's authority under 5 U.S.C. 601(4), NCUA has determined that small credit unions are those with less than one million dollars in assets. See 12 CFR 791.8(a). NCUA's final rule will apply to approximately 1,624 small credit unions.

At the time of issuance of the proposed rule, NCUA could not make a determination for certification. Therefore, NCUA issued an IRFA pursuant to section 603 of the

Regulatory Flexibility Act. After reviewing the comments submitted in response to the proposed rule, the NCUA certifies that this final rule for establishing guidelines for safeguarding member information will not have a significant economic impact on a substantial number of small entities.

Two commenters specifically responded to this issue. Both indicated that the guidelines may be too burdensome for small credit unions, and suggested that a different set of standards should apply to small credit unions whose member information is not accessible to the outside to reduce the burden and paperwork. The comment letters do not provide the NCUA data to quantify the costs of implementing the requirements of the final guidelines.

The NCUA anticipates the compliance costs will vary across credit unions. However, safeguarding member information is a vital aspect of the ongoing business operations of all credit unions. The potential cost to a credit union's reputation caused by lack of member confidence necessitates secure systems for a credit union to remain competitive.

The final guidelines implement the provisions of Title V, Subtitle A, section 501 of the GLB and apply to all financial institutions. The NCUA has attempted to minimize any significant economic impact on a larger number of small credit unions. This final rulemaking does not substantively change existing statutory requirements or represent any change in the policies of the NCUA, but provides appropriate standards relating to the security and confidentiality of member records. Nor do the final guidelines substantively change existing information system guidance. The final guidelines were designed to be consistent with security-related supervisory guidance previously issued by the NCUA and the FFIEC.

Consequently, the NCUA believes these guidelines represent minimum standards for protecting member information and are consistent with current practices among most credit unions. Further, NCUA believes the changes made to the final rule enhance its flexibility for small credit unions, based on their own risk assessment and complexity of services. For these reasons the final guidelines will not have a significant economic impact on a substantial number of small credit unions, and a final regulatory flexibility analysis is not required.

C. Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their regulatory 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. This final rule applies to all federally-insured credit unions, but it does not have substantial direct effect on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined the final rule and appendix does not constitute a policy that has federalism implications for purposes of the executive order.

D. Treasury and General Government Appropriations Act, 1999

NCUA has determined that the proposed rule and appendix will 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).

E. Small Business Regulatory Enforcement Fairness Act

The Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104-121) provides generally for congressional review of agency rules. A reporting requirement is triggered in instances where NCUA issues a final rule as defined by section 551 of the Administrative Procedures Act. 5 U.S.C. 551. NCUA is recommending to the OMB that it determine that this is not a major rule, and awaits its determination.

V. Agency Regulatory Goal

NCUA's goal is clear, understandable regulations that impose minimal regulatory burden. No commenters addressed this particular request for comments.

List of Subjects in 12 CFR Part 748

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

By the National Credit Union Administration Board on January 18, 2001.

_____
Becky Baker
Secretary of the Board

For the reasons set forth in the preamble, the NCUA Board amends 12 CFR part 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 is revised to read as follows:

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

2. Heading for Part 748 is revised as set forth above.

3. 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 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) assist in the identification of persons who commit or attempt such actions and crimes; and

(4) prevent destruction of vital records, as defined in 12 CFR part 749.

4. Add Appendix A to Part 748 to read as follows:

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.

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.”

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. Member means any member of the credit union as defined in 12 CFR 716.3(n).

b. 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.

c. Member information system means any method used to access, collect, store, use, transmit, protect, or dispose of member information.

d. 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; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member. 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.

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.