

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

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

D. Address and mitigate harm to individual members.

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

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

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

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

The proposed Guidance provides that a credit union should notify each affected member when it becomes aware of unauthorized access to sensitive member information, unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur, and takes appropriate steps to safeguard the interests of affected members, including monitoring affected members' accounts for unusual or suspicious activity. For the purposes of the proposed Guidance, NCUA defines sensitive member information to mean a member's social security number, personal identification number (PIN), password, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. Sensitive member information would also include any combination of components of member information that would allow someone

to log onto or access another person's account, such as user name and password.

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

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

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

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

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

The proposed Guidance also describes other forms of assistance that financial institutions have offered to their

customers in incidents of this type. Credit unions may wish to offer such forms of assistance to their members and describe them in the member notice.

II. Request for Comments

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

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

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

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

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