

immediately notify, by telephone, appropriate law enforcement authorities and NCUA or its primary state regulator, in addition to filing a timely SAR.

### C. Contain and Control the Situation

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

### D. Corrective Measures

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

#### 1. Flag Accounts

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

#### 2. Secure Accounts

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

#### 3. Member Notice and Assistance

Under part 748 and appendix A, a credit union's security program must be designed to protect its members' information against unauthorized access or use. A credit union should not forgo notifying its members of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so. Under the circumstances described in appendix A, the credit union should notify and offer assistance to members whose information

was the subject of the incident.<sup>16</sup> If the credit union is able to determine from its logs or other data precisely which members' information was accessed or misused, it may restrict its notification to those individuals. However, if the credit union cannot identify precisely which members are affected, it should notify each member in groups likely to have been affected, such as each member whose information is stored in the group of files in question.

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

*b. Content of Member Notice*—The notice should describe the incident in general terms and the member's information that was the subject of unauthorized access or use. It should also include a number that members can call for further information and assistance. The notice also should remind members of the need to remain vigilant, over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft.

*Key Elements:* In addition, the notice should:

- Inform affected members that the credit union will assist the member to correct and update information in any consumer report relating to the member, as required by the Fair Credit Reporting Act;
- Recommend that the member notify each nationwide credit reporting agency to place a fraud alert<sup>17</sup> in the member's consumer reports;
- Recommend that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- Inform the member of the right to obtain a credit report free of charge, if the member has reason to believe that the file at the consumer reporting agency contains inaccurate information due to fraud, together with contact information regarding the nationwide credit reporting agencies; and
- Inform the member about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft, and encourage the member to report any incidents of identity theft to the FTC. The notice should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.<sup>18</sup>

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

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

<sup>17</sup> A fraud alert will put the member's creditors on notice that the member may be a victim of fraud.

<sup>18</sup> Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) and 1-877-IDTHEFT.

- Provide a toll-free telephone number that members can call for assistance;
- Offer to assist the member in notifying the nationwide credit reporting agencies of the incident and in placing a fraud alert in the member's consumer reports; and
- Inform the member about subscription services that provide notification anytime there is a request for the member's credit report or offer to subscribe the member to this service, free of charge, for a period of time.

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

### III. Circumstances for Member Notice

#### Standard for Providing Notice

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

#### Sensitive Member Information

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

#### Examples of When Notice Should Be Given

A credit union should notify affected members when it is aware of the following incidents unless the credit union, after an appropriate investigation, can reasonably conclude that misuse of the information is

<sup>14</sup> See FFIEC Information Security Booklet, Dec. 2002, pp. 68–74.

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

<sup>19</sup> [www.occ.treas.gov/idtheft.pdf](http://www.occ.treas.gov/idtheft.pdf);  
[www.federalreserve.gov/consumers.htm](http://www.federalreserve.gov/consumers.htm);  
[www.ftc.gov/consumers/consumer/news/cnsum00/idthft.html](http://www.ftc.gov/consumers/consumer/news/cnsum00/idthft.html).