



DCU BULLETIN

Division of Credit Unions

Washington State Department of Financial Institutions

Phone: (360) 902-8701

Toll-Free FAX: 877-330-6870

September 22, 2005

No. B-05-06

Guidance When Data Security Systems Are Breached

It is possible that unauthorized access to your credit union's member personal information may occur, even though your credit union has taken steps to secure and protect the information technology systems from internal and external breaches. Generally those steps include actions to assure that third party service providers are protecting your member's personal information, actions to conduct satisfactory testing of your credit union's systems (including penetration testing), and other important steps to minimize the threat of a security breach. This Bulletin provides information about recently adopted rule and law changes, as well as regulatory guidance that will help your credit union develop a security response system to properly respond to security breach incidents.

New Washington State Law

A new section of state law, RCW 19.255.010 (see Appendix I), has been adopted, effective July 24, 2005, that will affect businesses that own computerized data, which includes personal information¹. This new RCW provides for member notification, "without unreasonable delay," in the event of breach of data security.

The negative impact of a security breach incident could be devastating if management is not ready to respond quickly with a well thought out plan. Therefore, your credit union should have a response plan in place and should have tested it to an appropriate level.

Final Rule Amendments to 12 CFR 748

On June 1, 2005, the final NCUA rule amendments to 12 CFR 748 became effective. 12 CFR 748 was amended to require that every federally insured credit union have a security program that contains a provision for responding to incidents of unauthorized access to member information. Appendix B of Part 748, entitled Guidance on Response Programs for Unauthorized Access to Member Information and Notice, which is included in the final rule amendments will assist credit unions in developing and maintaining their response programs. Appendix B states the expectation that every federally insured credit union will develop a

¹ See the attached state law change (RCW) for definition of personal information.

response program that includes member notification procedures to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to the member. The following link will take you to the final rule, 12 CFR 748 and Appendix B. Note: Appendix B begins on page 79.

<http://www.ncua.gov/RegulationsOpinionsLaws/RecentFinalRegs/F-748.pdf>.

To provide greater assurance of compliance with the RCW, the Division of Credit Unions (Division) recommends credit unions use the NCUA Rule as a sound framework for properly protecting your credit union in case of an unauthorized breach of your member's information. Part 748 Appendix B was established to fulfill a requirement in Section 501b of the Gramm-Leach-Bliley Act in which Congress directed Agencies to establish standards for financial institutions to ensure the security and confidentiality of customer records and information. **The amendments to 12 CFR 748 may not agree perfectly with the recently adopted RCW. Credit unions will need to carefully evaluate both to ensure the best protection for their operations.**

Response Program Elements

Part 748 Appendix B states a response program should contain the following five components:

1. Assess the Situation

Management must be able to quickly set in motion a response team that can efficiently assess the situation and who can accurately determine the cause and extent of the security breach. This team will need to accurately identify what information systems and customer information may have been compromised.

2. Notify Regulatory Agencies

Your credit union should notify the NCUA Regional Director and the Division of Credit Unions promptly after management has found out about a security breach involving unauthorized access to or use of sensitive information. Notification to the Division should occur within one business day after your credit union discovers the security breach and may be made via e-mail at dcu@dfi.wa.gov or via telephone at (360) 902-8701. Please do not send sensitive information by e-mail which may be released to comply with Washington State government public records requirements. It will be best to talk to us before sending sensitive information about the securities breach. When the media calls us, it is helpful to be able to explain the steps you are taking to address the situation.

3. Notify Law Enforcement Agencies

Notify appropriate law enforcement authorities using the Suspicious Activity Report. Certain situations involving ongoing federal criminal violations may require additional notifications.

4. Contain and Control the Situation

The responsive actions taken to contain and control the incident and to prevent further unauthorized access to or use of customer information are vitally important. All actions should consider proper preservation of records and other evidence. This may require that your credit union do the following:

- a) Shut down applications or third party connections;

- b) Reconfigure firewalls;
- c) Change computer access codes;
- d) Modify physical access controls;
- e) Place additional controls on service provider arrangements; and
- f) Ensure all known vulnerabilities in your credit union's computer systems have been addressed.

5. Notify Members When Warranted

After a security breach is found, credit unions may need to take action to reduce potential harm to its members through direct notification of the members. Determining how your credit union can best respond will be challenging. **Please review the new RCW and Part 748 Appendix B for variations in the definition of "personal information."**

Notification Requirements and Exceptions

One of the key points in the new RCW involves the notification of members when security over personal information has been breached. The new section of the RCW also provides for certain circumstances under which notification may not be necessary. This Bulletin will not attempt to restate the requirements identified in RCW. Credit unions are strongly encouraged to understand those circumstances and how they may apply.

Part 748 Appendix B provides a standard for notification that may satisfy the safe harbor provision in Section 2(8) of the new RCW. **When following the Appendix B standards, a credit union should exercise caution to ensure they remain compliant with RCW 19.255.010.**

Member notice should be timely, clear, and conspicuous, and be delivered in a manner that will ensure the customer is likely to receive it. The notice should describe the incidence in general terms and state the customer's information that was subject to unauthorized access. It should also include a number that members can contact for further information and assistance. The key elements of the notice should include:

- a. A recommendation that the member review account statements and immediately report any suspicious activity to the credit union;
- b. A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;
- c. A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- d. An explanation of how the member may obtain a credit report free of charge; and
- e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.

Responding to Members After the Notice has Been Sent

The public is extremely sensitive to the disclosure of personal information. You should anticipate that members may be upset and that your credit union may be inundated with telephone calls, e-mails, and other inquiries regarding the notice they receive. Management must anticipate the resources (mainly human) that will be needed to adequately respond to these inquiries. Staff will need to be satisfactorily trained to respond to member concerns. Specifically, credit union personnel will need training on how to advise customers on placing a “fraud alert” on the credit reporting system for themselves or in more extreme instances place a “block” on their credit reports. Also, staff will need to know how to secure the accounts of members. Your credit union should be able to quickly put this training in place.

Implementing Protective Actions

After a security breach is found, credit unions will need to take action to reduce potential harm to its members. Determining how your credit union can best respond to security breaches will be challenging. We encourage you to take the following actions:

- a) **Flag accounts** – The financial institution should immediately identify and monitor affected accounts for unusual activity and implement controls for unauthorized withdrawal or transfer of funds.
- b) **Secure accounts** – When a personal identification number (PIN) password or other unique identifier on an account has been misused, the financial institution should secure the account and all other related accounts and credit union services for that member.
- c) **Provide customer notice** – When necessary as provided in the RCW and Part 748 Appendix B.

Third Party Service Providers

Every credit union should require (by contract) its service providers to implement appropriate measures designed to protect against unauthorized access to member information. Your credit union’s contracts with its third party service providers should require the service providers to fully disclose to you any security breach(es) resulting in unauthorized intrusion into your credit union’s member information systems maintained by the service provider. These contractual obligations need to require the service providers to take appropriate actions that are consistent with your credit union’s policies to address incidents of unauthorized access to member’s financial information. This will enable your credit union to expeditiously implement its response program. We recommend that an attorney review each third party contract.

Data Encryption

You may be wondering whether data encryption alone is sufficient to protect member information. The short answer is data encryption is important, but it is only one important tool in assuring that nonpublic member information is properly secured. Encryption provides another level of security, if the encryption is done to the level of sophistication and control that would make it highly unlikely that data could be unencrypted and used. If encrypted personal member information is stolen, and the encryption is such that misuse of the information is unlikely, then a security breach notice may not be necessary.

How to Adequately Monitor for and Find Security Breaches

Security breaches are often identified when an employee notices unusual computer activity including; unusually slow response times, a displayed message, missing files, or programs that no longer function properly. When a breach is detected in this manner, significant damage from the breach may have already occurred.

It is far better for credit unions to actively monitor systems to detect the first stages of a breach. This is accomplished through the recording and review of system security events. Firewalls and servers have the ability to record and report security events. Credit unions should take advantage of their systems ability to record events and should implement a regular and routine review of these events by personnel with the competency to analyze the data.

Credit unions can also turn to vendors that provide security monitoring of systems. These vendors provide Intrusion Detection (IDS) or Intrusion Prevention (IPS) services. An IDS or IPS service typically involves the placement of a sensor (a computer designed to detect a breach) on the credit union's network. The vendor then monitors the sensor and provides useful reporting and alerting capabilities so attempted breaches are detected quickly and responded to appropriately.

IS&T Examiners Begin Reviewing Response Preparedness

On October 31, 2005, the Division IS&T examiners will begin reviewing credit union's response preparedness during the regularly scheduled safety and soundness examinations. We are anticipating that response preparedness plans will be adapted to the size and resources of individual credit unions. For example, we would anticipate that credit unions over \$100 million in assets would have a separate Incident Response Plan rather than a section in the Information Security Policy. Smaller credit unions response preparedness plans may rely more on previously identified and qualified service providers rather than their own staff to handle much of the necessary response.

Please contact Doug Lacy-Roberts at (360) 902-0507, if you have any questions about this Bulletin.

Appendix I

RCW 19.255.010

Disclosure, notice--Definitions--Rights, remedies.

(1) Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(2) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(5) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(7) For purposes of this section and except under subsection (8) of this section, "notice" may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) E-mail notice when the person or business has an e-mail address for the subject persons;

(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and

(iii) Notification to major statewide media.

(8) A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(9) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

(10)(a) Any customer injured by a violation of this section may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this section may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(d) A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

[2005 c 368 § 2.]

NOTES:

Similar provision: RCW [42.17.31922](#).