STATEMENT

OF

ROBERT M. FENNER

GENERAL COUNSEL
NATIONAL CREDIT UNION ADMINISTRATION

"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"

BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

U.S. HOUSE OF REPRESENTATIVES

MAY 18, 2005

"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"

Chairman Bachus, and Members of the Subcommittee, I appreciate your invitation to present this testimony reviewing the National Credit Union Administration's (NCUA's) experiences with information systems and technology (IS&T) incidents and other security events resulting in the potential compromise of personal financial data. We also identify actions by NCUA to ensure credit unions safeguard member information and to mitigate potential losses to credit unions and members when breaches occur. We recommend that NCUA be granted examination authority over third party vendors, which would enable us to better monitor risk and protect credit union members' personal financial data.

Examples of Data Security Breaches Involving Credit Union Members

Information is provided here on types of security breaches NCUA and credit unions have experienced. These security breaches include: fraudulent email or telephone scams, known as phishing; the unauthorized storing of customer information and the ensuing theft of this information; the theft of a credit union's hard drive; and the theft of a vendor's computer. We also provide information on how NCUA and credit unions have responded to these data security incidents.

Phishing Scams

In a typical phishing scam, a false email is sent asking the recipient to click on a link to verify his or her credit union account registration. If the recipient proceeds to do so, the link directs him or her to a false website and asks for the member's credit union account number and PIN, along with other personal information. At least eight credit unions, NCUA itself, and a national credit union trade association have been affected by such fraudulent email or telephone scams to obtain personal financial information.

Later in this testimony, we describe applicable federal laws and the regulations and other guidance NCUA has issued prescribing how credit unions must respond to data security breaches, including phishing. When phishing incidents have occurred in the past, NCUA has followed and has recommended credit unions and other affected entities follow a three-prong response.

First, the affected entity should alert the regulators, the industry, and potential victims about the fraud. This notice occurs through website postings, and notices to staff, state supervisory authorities, and credit unions. These notifications are picked up by the credit union press and further disseminated to the general public. Second, the affected entity should do what it can to shut down the scam, which, for example, could be a bogus website. This could occur by notifying the internet service provider who in turn would proceed to immediately shut down the

bogus website. Third, the affected entity should gather as much information as it can and refer the scam to the appropriate law enforcement authorities, such as the FBI, the Department of Justice's Cybercrimes Unit, and the United States Secret Service.

Lawsuit versus B.J.'s Wholesale Club, Inc.

Another data security breach involving credit unions and their members is reflected in a pending civil lawsuit filed April 4, 2005 by the CUNA Mutual Group against B.J.'s Wholesale Club, Inc., in Massachusetts Superior Court. The CUNA Mutual Group is a mutual insurance company and provider of fidelity bonds and other financial services to credit unions and their members. CUNA Mutual seeks recovery for approximately $4.5 million in losses on behalf of itself and 163 credit unions who are bond policyholders.

The lawsuit alleges that B.J.'s Wholesale Club used point of sale software systems that captured and stored its customers' full magnetic strip information from their credit and debit cards after authorizing transactions. The storing of the information was in violation of the Visa and MasterCard association rules. In March 2004, a security breach committed by an unknown hacker occurred, compromising approximately 40,000 credit and debit cardholders and their related personal financial information.

The lawsuit alleges that a substantial number of credit union members had used their cards at B.J.'s and that they are now at greater risk for identity theft and for criminals to use the data to make duplicate cards to engage in fraudulent transactions. The alleged losses include fraud losses that credit unions have incurred and are unable to collect, the blocking costs for the affected cards, and expenses for reissuing affected cards.

Theft of Credit Union's Hard Drive

Another example of a breach of credit union members' data security involved a state-chartered credit union in California. During the weekend of November 15, 2003, two offices at the credit union were vandalized and a hard drive was taken. The hard drive was from the loan manager's PC. The credit union was preparing for a loan pre-approval promotion and member data had been downloaded from the mainframe computer to the PC and was being analyzed for the promotion.

Initially management believed approximately 49,000 member's names, account numbers, and social security numbers were on the hard drive. Further investigation disclosed almost 100,000 members whose data was compromised.

On Monday, November 17, 2003, the credit union contacted the local police and secret service and an investigation was begun. The credit union's investigation showed a lack of control over access to the building while remodeling was

occurring over the weekend. Furthermore, the investigation revealed a lack of properly placed security cameras and a lack of controls over the credit union's electronic card keys.

The credit union sent a letter disclosing the compromise to all affected members on November 19. The credit union also hired additional staff and temporarily reorganized the call department to field the anticipated calls from members. Initially, call volume was very high but rapidly tapered off as the credit union explained what it was doing to protect the members against misuse of their personal information. To provide additional protection to members against potential fraud and identity theft, the credit union subscribed to the credit tracking system provided by the credit bureaus for one year. This allowed the credit union to review monthly reports to check for unusual activity in its members' accounts.

After the theft, the credit union reissued new electronic key cards to employees and a methodology was implemented to keep track of who had the cards and what areas they could access. The credit union moved its security cameras and added additional ones to the building's entrances. The credit union established new procedures to monitor outside contractors. The credit union revised the data processing system and installed on every PC a program that bars downloading of member data to the PC. Instead, all analysis, such as for a loan promotion, is done on a portion of the mainframe.

The cost to the credit union was substantial, not only in direct costs, but also in the amount of staff time, from the tellers to the CEO, allocated to the issue. Some months the costs exceeded 50% of net income. There are no known losses to the members relating to the theft.

Theft of Vendor's Computer

The following is a summary of the events surrounding the theft of member data of a state-chartered credit union in Washington State. The credit union had used the services of PSB, The Marketing Supersource (PSB) for mailing of marketing materials to select credit union members since mid-year 2003. Two promotional material mailings, a home-equity loan offer and credit card offer, were handled by PSB in May 2004.

A burglary of PSB's office in Lake Forest, California occurred during the night of July 8 or morning of July 9, 2004. A computer that could be easily seen from the office window was stolen. The computer was used to store member information while PSB worked on credit union promotions. PSB could not determine what information was stored on the stolen computer because it did not have a recent back-up tape of the computer; nor could it verify if PSB users had deleted the credit union's member information after a promotion was completed. There was no evidence that the computer had been targeted for the information it contained.

On July 27, 2004, 18 days after the theft, PSB notified the credit union that member information might have been compromised. The information for 13,100 members, including names, addresses, and social security numbers, was possibly stored on the PSB computer. The Washington credit union management immediately assembled an incident response team to determine potential risks and necessary actions.

On August 2, 2004, the credit union mailed letters to all 13,100 affected members informing them of the theft and encouraging members to contact the three major credit reporting agencies and place a "Fraud Alert" with each credit reporting agency. The credit union sent members additional information to advise them to remain vigilant over the next 12 to 24 months to monitor their credit report and account activity and, if they desired, to immediately call the credit union to place a password on their account. The credit union attempted to assure members of its priority in keeping member information secure and set up a toll free number to address member concerns. As of August 17, 2004, the credit union had received over 30 letters, 5,000 phone calls, and numerous email messages from members expressing their concerns and frustrations.

On August 17, 2004, the Washington State Division of Credit Unions completed an onsite investigation of this incident. As a result, the credit union learned that its marketing department was not complying with the credit union's data security procedures. The credit union also implemented the following recommendations from the investigation:

- Maintain written contract/agreements with vendors;
- Perform and document a member information security risk assessment according to 12 C.F.R. Part 748. Update the risk assessment annually and whenever significant system changes occur. Report to the Board at least once ever year;
- Document information supplied to vendors/service providers;
- Monitor service providers;
- Require reporting from service providers to appropriately evaluate the service provider's performance and security;
- Control information supplied to service providers, ensuring that the information is managed and secured properly; and
- Encrypt electronic member information, including while in transit or in storage on networks or systems in which unauthorized individuals may have access.

There has been no evidence of fraud as a result of the member data theft.

Current Laws and NCUA Actions, Including Regulations, Guidance and Examination Procedures

The primary current federal laws governing data security for credit unions are found in the Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. §6801(b), and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. No. 108-159. NCUA has promulgated regulations under these laws containing requirements for credit unions to enhance data security, including Fair Credit Reporting Act regulations, 12 C.F.R. Part 717, and Security Program regulations in 12 C.F.R. Part 748.

GLBA 501b Regulations

Under the GLBA, section 501b, NCUA and other federal financial regulators were required to establish technical standards for financial institutions to meet the following objectives: one, ensuring the security and confidentiality of member records; two, protecting against anticipated threats or hazards to the security or integrity of such records; and three, protecting against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member.

Accordingly, NCUA, in consultation and coordination with the other federal financial regulators, amended its existing Security Rule, 12 C.F.R. Part 748, in 2001 to require that a federally-insured credit union's security program contain elements to meet these objectives. Appendix A of Part 748 provides guidance in developing and implementing an information security program. 66 Fed. Reg. 8152 (January 30, 2001).

Stemming from the growing number of security breaches in the financial services sector involving access to customer information, NCUA, again in consultation and coordination with the other federal financial regulators, further amended Part 748 in 2005, effective June 1, 2005. 70 Fed. Reg. 22763 (May 2, 2005). In this change, NCUA outlined its expectations that each credit union develop and maintain a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of member information. Appendix B describes the components of a response program, including procedures for notifying members about incidents of unauthorized access to or use of member information that could result in substantial harm or inconvenience to the member.

The new guidance provides that, when a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. The guidance states that if the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible. The credit union may delay the notice if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. Under the guidance, the credit union should notify its primary

regulator of a security breach involving sensitive member information, whether or not the credit union notifies its members.

Fair and Accurate Credit Transactions Act of 2003 (FACTA)

Complementing the GLBA's requirements implemented in Part 748, FACTA established new requirements and protections for credit unions and their members relating to data security. Originating with the Committee on Financial Services, FACTA amended the Fair Credit Reporting Act (FCRA) to: help consumers combat identity theft; establish national standards for the regulation of consumer report information; assist consumers in controlling the type and amount of marketing solicitations they receive; and restrict the use of sensitive medical information.

Disposal Rule

NCUA coordinated with the other federal financial regulators and issued a final rule on the Proper Disposal of Consumer Information under FACTA §216, to address the risks associated with identity theft. Under the final rule, effective December 29, 2004, federal credit unions must take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. 69 Fed. Reg. 69269, (Nov. 29, 2004); 12 C.F.R. Parts 717 and 748.

The standard for disposal is flexible to allow credit unions to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time. Federal credit unions are expected to implement these measures consistent with the provisions in NCUA's Guidelines for Safeguarding Member Information under Part 748, Appendix A.

The disposal rule includes specific examples of appropriate measures that would satisfy its disposal standard, both for paper and electronic records. For example, an appropriate measure would be requiring the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed. For electronic media, an appropriate measure would be requiring the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed. In addition, it would be an appropriate measure if, after due diligence, a credit union enters into and monitors compliance with a contract with another party engaged in the business of record destruction to properly dispose of the consumer information.

FACTA Regulatory Alert and Interagency Legal Opinion Letter

NCUA issued a Regulatory Alert in January 2005, 05-RA-03, Fair and Accurate Credit Transactions Act of 2003, that lists and discusses key provisions of FACTA. A copy of Regulatory Alert 05-RA-03 is attached and also available on NCUA's website at: http://www.ncua.gov/reg_alerts/2005/05-RA-03.doc. In addition, NCUA, the federal banking agencies, and the FTC jointly issued an interagency legal opinion letter offering guidance on FACTA compliance. This letter is also attached and available to the public on NCUA's website under Legal Opinion Letter 04-1140, dated November 24, 2004, http://www.ncua.gov/RegulationsOpinionsLaws/opinion_letters/2004Letters.htm.

The FACTA Regulatory Alert and Legal Opinion Letter 04-1140 both identify provisions of FACTA relating directly to handling IS&T and other data security issues, either before or after a breach has occurred. Certain FACTA provisions must be implemented by regulations or guidance adopted by federal regulators. NCUA, with other federal financial agencies, is currently actively engaged in developing guidance or rules as appropriate to implement these FACTA provisions and training credit unions and examiners.

For example, NCUA, the FTC and the federal banking agencies are participating in ongoing interagency meetings to draft a proposed Red Flags rule establishing guidelines for identifying, mitigating and preventing identity theft. FACTA §114; FCRA §615(e). The Red Flags rule will likely require credit unions to develop, implement, and monitor identity theft protection policies and procedures. The agencies also plan to issue another FACTA proposed rule to prevent identity theft on the requirement to reconcile addresses simultaneously with the proposed Red Flags rule. FACTA §315; FCRA §605(h). These regulations, once finalized, will further enhance the safeguarding of member data.

The FACTA Regulatory Alert and Legal Opinion Letter both also identify certain provisions of FACTA that became effective December 1, 2004 and do not depend on agency rulemaking. These provisions include, for example, fraud and active duty alerts, blocking of information resulting from identity theft, prevention of repollution of consumer reports, and disclosure of credit scores. Credit unions are developing compliance procedures, modifying systems, and training staff to implement the new requirements. These requirements will serve to safeguard member data and provide assistance to members whose data has been compromised or who are the victims of identity theft.

For example, the repollution provision of FACTA requires that, when reporting data to consumer reporting agencies, credit unions must have reasonable procedures to stop re-reporting data derived from identity theft transactions upon notification of identity theft by a member or consumer reporting agency (CRA). FACTA §154(a); FCRA 623(a)(6). Reasonable procedures means procedures that provide reasonable assurance that data related to an identity theft transaction will not be reported to a consumer reporting agency, once a consumer provides notification of identity theft.

We note that acceptable procedures could vary, depending on the size and complexity of a credit union. For example, a large credit union with an automated system for reporting to CRAs should be able to flag and stop reporting identity theft transactions within hours of notification. A smaller credit union that manually submits weekly reports to the CRAs might take seven days (until the next weekly report) to update records.

While the process and procedures will vary among institutions, every credit union that reports to CRAs should take the time to establish and document, in writing, the process that will be used. In addition to strong policy and internal controls, under FACTA, NCUA has advised credit unions that during the ongoing review of internal controls, a supervisory committee member could check a sample of credit reports to confirm that identity theft information was not accidentally re-reported.

Interagency Examination Guidance and Enforcement

NCUA is currently working with a FFIEC group to draft interagency examination procedures for FACTA, prepare training modules for examination staff that will also be made available to the public, and an examiner questionnaire will be developed, based on the interagency exam procedures. By using interagency procedures, the FFIEC agencies will be able assure consistent application of FACTA provisions across all financial institutions. Should a deficiency in compliance with FACTA be noted, NCUA would work with the credit union to ensure appropriate corrections are made. NCUA will enforce FACTA like other consumer compliance regulations, such as Truth in Lending (Reg Z) and Truth in Savings (Reg DD).

Public Education and Letters to Credit Unions

In 2004, the NCUA Chairman JoAnn Johnson was appointed to the U.S. Financial Education and Literacy Commission. NCUA is a key partner with the Treasury Department on financial education initiatives, such as educating consumers on data security issues and identity theft. Credit unions also have made ongoing efforts to communicate with members about identity theft and how to protect themselves from having their identity stolen.

Moreover, FACTA imposes responsibility for the establishment and implementation of a public education campaign concerning identity theft on the FTC. NCUA and credit unions commonly refer victims of identity theft to the FTC web site, where there is a comprehensive discussion of identity theft issues. Included on the FTC website, for example, is a model summary of rights for identity theft victims. FTC developed the model summary as required under the FCRA §609(d). During the development process, FTC solicited feedback from federal financial regulators, including NCUA. We note that the FTC FACTA

manager and NCUA staff have regularly been working together, participating on lecture panels, and training credit union representatives on FACTA implementation.

In addition, NCUA has made public, through web-site posting, guidance documents addressing identity theft, which were sent to credit unions. NCUA has issued at least 30 Letters to Credit Unions related to identity theft and other IS&T data security risks, issues, and concerns, a list of which is included as an appendix. Some example of NCUA letters include:

• In May 2000, NCUA published Letter to Credit Unions 00-CU-02, Identity Theft Prevention. The Letter discussed the rising frequency of identity theft and encouraged credit unions to take precautions to deter the theft of member information. A best practices guide and reference information from the National Summit on Identity Theft were provided as enclosures.

• In September 2001, NCUA published Letter to Credit Unions 01-CU-09, Identity Theft and Pretext Calling. The Letter discussed identity theft issues and included a brochure, How to Avoid Becoming a Victim of Identity Theft, that credit unions were encouraged to share with their members.

• In August 2003, NCUA published Letter to Credit Unions 03-CU-12, Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions. The Letter addressed fraudulent websites used to capture sensitive personal information with the intent to commit identity fraud.

• In April 2004, NCUA published Letter to Credit Unions 04-CU-05, Fraudulent Email Schemes. The Letter discussed identity theft issues related to deceptive emails requesting sensitive personal information.

• In September 2004, NCUA published Letter to Credit Unions 04-CU-12, Phishing Guidance for Credit Unions. This Letter discussed identity theft related to phishing and enclosed the FFIEC brochure on phishing. The brochure was made available to credit unions for distribution to their membership.

In addition, we note other steps NCUA has taken:

- NCUA has issued six Regulatory Alerts and one Information Systems & Technology Advisory dealing with IS&T related regulations.
- NCUA has issues four IS&T Security Alerts.
- NCUA representatives regularly speak on IS&T related issues at credit union conferences.
- NCUA has revised its IS&T examination program (examiner questionnaires) and is currently field testing those new questionnaires.
- NCUA modified its website to include a section devoted to IS&T.

Recommendations

One continuing area of concern to NCUA is our lack of examination authority to review the operations of third party vendors that provide services, such as loan processing and Internet banking, to credit unions. The Government Accountability Office (GAO) has noted this lack of authority on at least two occasions and recommended that NCUA pursue this issue with Congress.[1] The authority currently exists for the other federal financial institution regulatory agencies and it temporarily existed for NCUA prior to expiring on December 31, 2001. The authority has been effectively used to monitor risk, including data security risk, in third party vendors. In the absence of this authority, NCUA has occasionally experienced difficulty in obtaining the full cooperation of vendors, and in obtaining key documents, such as financial statements and audit reports. Accordingly, we continue to request that Congress consider a permanent restoration of NCUA's vendor examination authority.

Also, while credit unions and other financial institutions are carefully regulated with respect to the issue of data security as a result of GLBA and FACTA, the examples in the first part of my testimony raise the question whether merchants and other parties should be subject to comparable requirements. NCUA will be happy to work with the Subcommittee as you continue to consider whether additional Congressional action is advisable to improve the existing legal framework.

Attachments

[1] In a GAO Audit Report dated August 1999, the GAO noted several times that the expiration of NCUA's examination authority of third party service providers for Y2K, on December 31, 2001, would limit NCUA's future ability to effectively oversee third party firms that provide Internet financial services to credit unions. The report recommended NCUA pursue retaining this authority to maintain effectiveness in ensuring the safety and soundness of credit unions' electronic financial services.

According to a more recent GAO Audit Report, GAO-04-91, "Credit Union Financial Condition," dated October 2003: "unlike the other depository institution regulators, NCUA lacks authority to review the operations of third-party vendors, which credit unions increasingly rely on to provide services such as Internet banking. However, these third-party arrangements present risks such as threats to security of information systems, availability and integrity of systems, and confidentiality of information."

[From NCUA's website http://www.ncua.gov/IST/ISTltcu.html]

Related Letters to Credit Unions

NCUA is providing the following reference material to assist you with IS&T Issues.

LETTER #	TITLE	ENCL	DATE ISSUED
04-CU-14	Risk Management of Free and Open Source Software - PDF only	PDF only	11/04
04-CU-12	Phishing Guidance for Credit Union Members - PDF or MS Word	PDF Only	09/04
04-CU-09	ATMs: Triple DES Encryption in PDF or MS Word		4/ 2004
04-CU-06	E-Mail and Internet Related Fraudulent Schemes Guidance PDF or MS Word		5/ 2004
04-CU-05	Fraudulent E-Mail Schemes		4/ 2004
03-CU-14	Computer Software Patch Management	PDF	9/ 2003
03-CU-12	Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions		8/ 2003
03-CU-08	Weblinking: Identifying Risks & Risk Management Techniques		4/ 2003
03-CU-07	FFIEC Release of Information Technology Examination Handbook		4/ 2003
03-CU-05	Expanded AIRES Share and Loan Layout Specifications	FAQ For Share and Loan Record Layout	4/ 2003
03-CU-03	Wireless Technology		3/ 2003
02-CU-17	e-Commerce Guide for Credit Unions		12/ 2002
02-CU-16	Protection of Credit Union Internet Addresses		12/ 2002
02-FCU-11	Tips to Safely Conduct Financial Transactions Over the Internet - An NCUA Brochure for Credit Union Members		4/2002
02-CU-13	Vendor Information Systems & Technology Reviews - Summary Results		7/2002
02-CU-08	Account Aggregation Services		4/ 2002
01-CU-21	Disaster Recovery and Business Resumption Contingency Plans		12/2001
01-CU-20	Due Diligence Over Third Party Service Providers		11/ 2001

01-CU-12	e-Commerce Insurance Considerations		10/2001
01-CU-09	Identity Theft and Pretext Calling Brochure: How to Avoid Becoming a Victim of Identity Theft		9/2001
01-CU-11	Electronic Data Security Overview		8/2001
01-CU-10	Authentication in an Electronic Banking Environment		8/ 2001
01-CU-04	Integrating Financial Services and Emerging Technology		3/ 2001
01-CU-02	Privacy of Consumer Financial Information (with Enclosure)		2/2001
00-CU-11	Risk Management of Outsourced Technology Services (with Enclosure)		12/2000
00-CU-07	NCUA's Information Systems & Technology Examination Program	Zip of Excel Files Zip of Excel Files. (Revised August 7, 2002)	10/2000
00-CU-04	Suspicious Activity Reporting (see section regarding Computer Intrusion)		6/2000
00-CU-02	Identity Theft Prevention		5/2000
97-CU-5	Interagency Statement on Retail On-line PC Banking		4/1997
97-CU-1	Automated Response System Controls		1/1997
109	Information Processing Issues		9/1989