Testimony of

Glenn Strebe

President/CEO of Air Academy Federal Credit Union

On behalf of

The National Association of Federal Credit Unions

"Cyber Security"

Before the

House Small Business Committee

Subcommittee on Healthcare and Technology

United States House of Representatives

December 1, 2011

Introduction

Good afternoon, Chairwoman Ellmers, Ranking Member Richmond and Members of the Subcommittee. My name is Glenn Strebe, and I am testifying today on behalf of the National Association of Federal Credit Unions (NAFCU). Thank you for holding this important hearing. I appreciate the opportunity to share my views on cyber security and data security at our nation's credit unions.

I received my Bachelor of Science degree from the United States Air Force Academy and an Master's in Business Administration from Colorado State University. Since 1998, I have served as the President and CEO of Air Academy Federal Credit Union, headquartered in Colorado Springs, CO. AAFCU has $420 million in assets and serves more than 42,000 members in our 9 locations, as well as in student operated branches at two high schools. Previously, I served AAFCU's membership as the Chief Operating Officer and Chief Financial Officer. Prior to joining the credit union, I was an auditor and a financial analyst in the United States Air Force.

NAFCU is the only national organization that exclusively represents the interests of the nation's federally chartered credit unions. NAFCU is comprised of over 800 member-owned and operated federal credit unions. NAFCU member credit unions collectively account for approximately 62 percent of the assets of all federally chartered credit unions. NAFCU and the entire credit union community appreciate the opportunity to participate in this discussion on data security.

Background on Credit Unions

Historically, credit unions have served a unique function in the delivery of necessary financial services to Americans, including making business loans. Established by an Act of Congress in 1934, the federal credit union system was created—and has been widely recognized—as a way to promote thrift and to make financial services available to all Americans, including small businesses, who would otherwise have limited access to financial services. Congress established credit unions as an alternative to banks and to fill a precise public need—a niche that credit unions fill today for nearly 93 million Americans.

Every credit union is a cooperative institution organized "for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes." (12 U.S.C. §1752(1)). While more than 75 years have passed since the *Federal Credit Union Act* (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- Credit unions remain singularly committed to providing their members with efficient, low cost, personal service; and,
- Credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

The nation's approximately 7,200 federally insured credit unions serve a different purpose and have a fundamentally different structure than banks. Credit unions exist solely for the purpose of providing financial services to their members—while banks strive to make a profit for their shareholders, while also serving their customers. As owners of cooperative financial institutions

united by a common bond, all credit union members have an equal say in the operation of their credit union—"one member, one vote"—regardless of the dollar amount they have on account. These singular rights extend all the way from making basic operating decisions to electing the board of directors. Federal credit union directors also generally serve without remuneration—epitomizing the true "volunteer spirit" permeating the credit union community.

Today, credit unions continue to play a very important role in the lives of millions of Americans from all walks of life. As consolidation among financial depository institutions has progressed with the resulting de-personalization in the delivery of financial services by some large banks, the emphasis in consumers' minds has begun to shift not only to services provided but also—and in many cases more importantly—to quality and cost. While many large banks have increased their fees and curtailed customer service as of late, credit unions continue to provide their members with high quality personal service at the lowest possible cost. This has been evidenced most recently as thousands of Americans turned to local credit unions after several large national banks proposed new fee increases.

Protecting Consumer Information

NAFCU supports efforts to enact comprehensive data and cyber security measures to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 Gramm-Leach-Bliley Act (GLBA). Unfortunately, there is no comprehensive regulatory structure similar to what was put in place for financial institutions under GLBA for other entities that may handle sensitive personal and financial data. While NAFCU supports new measures to combat data breaches, any new legislation should

create a safe harbor for financial institutions already in compliance with GLBA; failing to do so would place an undue burden and cost on financial institutions that would be forced to retool systems that they already have in place.

Consistent with Section 501 of GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLBA and its implementing regulations have successfully limited data breaches among financial institutions. The best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. By and large, financial institutions, especially credit unions, have not been the source of significant data breaches. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

A Closer Look at the Gramm-Leach-Bliley Act

GLBA helped establish the current standard for financial institution consumer data privacy. GLBA places restrictions on the ability of financial institutions to share nonpublic personal information with nonaffiliated third parties. Under the Act, the definition of financial institution includes any entity offering financial products, including banks, insurance companies, securities houses, and credit unions. It should be noted that the GLBA was enacted at the dawn of the internet age, before many online payment systems became popular and, thus, not all are covered under this definition.

Specifically, the GLBA:

- Requires financial institutions to establish privacy policies and disclose them annually to their customers, setting forth how the institution shares nonpublic personal financial information with affiliates and third parties.
- Directs regulators to establish regulatory standards that ensure the security and confidentiality of customer information.
- Permits customers to prohibit financial institutions from disclosing personal financial information to non-affiliated third parties.
- Prohibits the transfer of credit card or other account numbers to third-party marketers.
- Prohibits pretext calling, which generally is the use of false pretenses to obtain nonpublic personal information about an institution's customers.
- Protects stronger state privacy laws and those not inconsistent with these federal rules.
- Requires the U.S. Department of Treasury and other federal regulators to study the appropriateness of sharing information with affiliates, including considering both negative and positive aspects of such sharing for consumers.

The Act also imposed an affirmative obligation on financial institutions to respect their customers' privacy interests. In general, the Act permits financial institutions to share information with third parties selling financial products (e.g., insurance or securities) provided certain requirements are met. Financial institutions may continue such joint marketing practices without being subject to opt-out provisions of the legislation, provided they disclose the practice to their consumers and members and enter into a confidentiality agreement with the third party.

GLBA requires credit unions to provide clear and conspicuous privacy notices to members. The language must be understandable and written in a manner to let the reader know the purpose and significance of the notice. Furthermore, the privacy notices must accurately reflect the practices of the credit union. These annual privacy notices constitute a major compliance cost.

State laws are not superseded, altered, or affected, except to the extent that it is inconsistent with the federal privacy regulations. A state statute, regulation, etc., is deemed consistent with the privacy regulations if the FTC determines that it provides a consumer greater protection than those provided under the privacy regulations. For all practical purposes, a more protective state law will supersede GLBA protections.

Pursuant to section 508 of GLBA, the Treasury conducted a study of information sharing practices among financial institutions and their affiliates and came to five general conclusions:

- First, financial services providers and their customers have a strong interest in promoting the security of personal financial information that is following prudent practices so that information is used for the benefit rather than the harm of the customer.

- Second, the sharing of information, within secure parameters reinforced by uniform national standards, has increased the access of more consumers to a wider variety of financial services, at lower costs, than ever before.

- Third, the growing problem of fraud through identity theft not only disrupts the lives of individuals and families, but it also tears at the fabric of commerce in our information age.

- Fourth, in our technology-based economy, so dependent upon accurate, timely information, current uniform national standards for information sharing have proven as essential to fighting identity theft as they are for economic growth and prosperity.

- Fifth, customers need to understand more easily and clearly the information-sharing practices of their financial institutions and how to exercise their say in how that information is shared in support of the customer relationship.

The GLBA addresses a number of key aspects of data security as outlined below.

Sensitive Consumer Information

Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log onto or access the member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

Unauthorized Access to Consumer Information

The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer 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 a member.

An information security program must begin with a comprehensive risk assessment to ensure that the policies, procedures and controls used to accomplish the institution's information security and privacy goals have enough depth and breadth to reach every impacted area within the organization. Technological solutions may represent part, or all, of the program depending on the needs of the institution. Such technological solutions may include two-factor authentication of user identities; firewalls and virus management strategies, error logs monitored continuously for attacks and attempted attacks.

Risk Assessment and Controls

The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

It is imperative that institutions understand that internal threats often times pose more of a threat to the institution and its members than hackers from the outside. With this in mind, the institution ensures strong hiring verification practices and incorporates training programs to promote a culture of compliance among its staff. At Air Academy Federal Credit Union, we have a number of internal control tests that we perform to train our employees on how to handle situations such as someone coming in dressed as a repairman trying to gain access to our server room.

Other issues are also important. For example, record retention, storage, and destruction is rapidly finding its way to the top of the compliance risk matrix. Similarly, business upgrades to their PCs have led to mass abandonment of computers whose files and hard drives not been sufficiently scrubbed to ensure data is irretrievable. Failure to adequately protect a member's identity when disposing of old records and/or old equipment may result in significant legal and compliance repercussions.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business.

At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to consumer information; and,
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies.
- Train staff to implement the credit union's information security program.
- 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."

Service Providers

The security guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to,

or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events, cost savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

An institution that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

Response Program

Every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers

Components of a Response Program

At a minimum, an institution's response program should contain procedures for the following:

- Assessing the nature and scope of an incident, and identifying what consumer information systems and types of consumer information have been accessed or misused
- Notifying its primary Federal regulator as soon as possible after the institution becomes aware of an incident involving unauthorized access to or use of sensitive consumer information, as defined below;
- Consistent with the agencies' suspicious activity report (SAR) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
- Taking appropriate steps to contain and control the incident to prevent unauthorized access to or use of consumer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and,
- Notifying customers or members when warranted.

Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

Consumer Notice

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good consumer relations, and enable

the institution's members to take steps to protect themselves against the consequences of identity theft.

Content of Consumer Notice

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the institution.

Delivery of Consumer Notice

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

Data Security at Air Academy Federal Credit Union

At Air Academy Federal Credit Union (AAFCU) we are relentless in our efforts to protect our members' sensitive data. The increased reliance on internet-based services has created new challenges and expenses over the last decade. With over 10,000 of our members living out-of-state, a large number of our transactions are performed online. In order to address this growing

trend, AAFCU has implemented and continues to execute security measures on many different levels. The following is a list of security components we use at AAFCU:

1. Firewall
2. Intrusion Prevention
3. Botnet Filtering
4. Anti-Virus protection
5. Malware protection
6. Management and Monitoring Services
7. Anti-Phishing and Phishing site takedown services
8. Third party vulnerability assessments and testing
9. Web Filter
10. Spam Filter
11. Secure Email
12. Encryption
13. End point security

Associated costs for Info Security Components:

1. Firewall, Intrusion Detection & Prevention (IPS/IDS) and Botnet Filtering: $4,000 *annually* for maintenance support. Initial procurement: $37,000;
2. 24/7 Monitoring of firewall; IPS/IDS and Botnet Filtering: $2900 *monthly;*
3. Firewall and server log collection/monitoring: Initial procurement: $33,500; support renewals: $5,000 *annually;*
4. Secure email and encryption: Initial procurement: $94,000; subsequent upgrades and maintenance since 2003: $81,000 (about $10,000 *annually*);
5. Anti-Virus and Malware protection: $3,000 *annually;*
6. End-point security and laptop encryption: $1500 *annually;*
7. Phishing take down services: $9,995 *annually;*
8. Web and Spam filters: $5,000 *annually; and,*
9. Third party vulnerability and penetration testing: $100,000 *annually.*

At AAFCU, we take our cyber security seriously. We use an "ethical hacker" that tests our security measures, looking for hidden vulnerabilities that need repair. All of our laptops and thumb-drives that are used on our systems are encrypted in case they ever fall into the wrong hands. We like to change penetration testing vendors as well as service providers every 2 to 3 years in order to avoid complacency and to keep a "fresh set of eyes" on our security system.

While all of these steps have a cost, we view them as best practices, especially for an entity that is serious about protecting their members' data.

For the record, our system has never been successfully hacked, and from our side, none of our members' sensitive data has ever been accessed by anyone without authorization. But despite much effort and expense to protect our members' sensitive data, the same information is routinely held by other entities that do not take the protection of sensitive data as seriously. Because the sensitive data is only as safe as the weakest link provides for, our members' data is often still vulnerable to hackers and thieves through the inadequate security systems of merchants, retailers, or other entities that store this type of consumer data.

The following is a list of estimated compromise totals within the last couple of years:

- 2009 – Cheers Liquors – over 200 cards involved – losses were just over $60,000.
- 2010 – Valero/Gas Stations – over 1600 cards involved – losses were just over $85,000.
- 2010/2011 – Michael's Store – over 200 cards involved – losses were just over $20,000.

In late 2010, we began to receive debit card compromise notices due to a data breach at the TJ Maxx/Home Goods database. In total, we had 3,100 member debit cards listed in the various compromise alerts. Over 2,000 letters were mailed out to members and we ultimately reissued 1,700 plastic cards. We calculated our expenses from this compromise (excluding labor) to be approximately $4,000.

Visa and TJX announced an alternative recovery program to help issuers to quickly and easily offset the costs incurred with this compromise. TJX will pay $41 million to Visa to fund this program. Our calculated settlement offer came to $1,370 – about 35% of our incurred expenses. Given the time and effort required to litigate directly against TJX, we will likely accept this settlement. Payment is contingent upon 80% of the issuer's accepting their respective offers. I imagine the vast majority will take the money and put the issue to rest.

Data Breach/Notification Proposals and Recommendations

Data breaches are a serious problem for both consumers and businesses. Financial institutions such as credit unions also bear a significant burden as they incur steep losses in order to reestablish member safety after a data breach occurs. The number and scope of data breaches are significant, and the damage realized is surprising.

For example, in 2009, the Heartland Payments Systems, a company that processes card payments for restaurants, retailers, and other merchants, disclosed that the computer the company used to process transactions had been compromised. Customer records for over 100 million payment card transactions per month, at nearly 175,000 merchants, were stolen. Millions of American consumers instantly became victims. Other infamous data breaches include an estimated 4.2 million credit and debit card numbers stolen from Hannaford Bros. grocery stores in the New England area in 2008, and retail giant TJX losing 94 million customer records in 2007.

More recently, on May 11, 2011, Michaels Stores, Inc. notified its customers that more than 90 terminals in 20 different states had been compromised in a debit card PIN scheme that may have compromised tens of thousands of customers' debit cards. This breach has been linked to hundreds of thousands of dollars in fraudulent cash withdrawals in California alone.

The emotional toll that a data breach can take on consumers is immense. Information and identities can be stolen, fraudulent account charges can occur, and credit scores can be damaged. Along with consumers, small financial institutions like credit unions also face financial burdens when fraud occurs. Credit unions are often forced to charge off fraud losses, which often stem from the failure of merchants to protect sensitive financial information about their customers or the illegal maintenance of such information in their systems.

In cases of data breaches or fraud, as demonstrated by the Michaels Stores breach discussed above, it is the credit union that must notify its members, issue new cards, change account numbers, and perform a host of other activities, all of which cost both time and money. The merchant who failed to protect the data is often undisclosed and unknown to the consumer and does not pay to make the consumer whole. Interchange fees have historically been one way the costs of such breaches were offset by merchants. However, recent Congressional action to limit debit interchange fees does not fully recognize this problem and will result in heavier burdens falling on financial institutions and consumers. Understanding the significance of debit

interchange to help offset data breaches at the hands of retailers and other entities that handle the same types of consumer information as financial institutions is critical.

Meanwhile, as cases of fraud become more prevalent, costs that credit unions pay for insurance, prevention services, and staff to handle member concerns continues to grow. As the volume of plastic card usage increases, so does the risk of data breaches and fraud.

The GLBA has worked for financial institutions and should serve as a model to extending greater data protections to other entities. In addition to complying with the GLBA, credit unions have been known to go above and beyond in helping their members navigate the steps they should take if they have been the victims of fraud. It should again be noted that there is no comprehensive regulatory structure similar to the GLBA for retailers, merchants, or others who collect or hold sensitive information.

NAFCU continues to seek enactment of comprehensive data security legislation in the 112th Congress and beyond. In the House, Rep. Mary Bono Mack (R-CA), Chairwoman of the Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade, introduced the *Secure and Fortify Electronic Data Act (H.R. 2577)*. The bill awaits action by the full committee. In the Senate, Tom Carper (D-DE) and Roy Blunt (R-MO) introduced, the *Data Security Act of 2011 (S.1434)*, a NAFCU-backed financial services approach to the issue, which has been referred to the Senate Banking Committee for further action. Both bills would require security

standards for different types of personal and account information, and require specific notification procedures in the event of a breach.

Additionally, Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, introduced the *Personal Data Privacy and Security Act of 2011*, which has been marked-up and placed on the Senate Legislative Calendar under general orders. Senator Leahy's bill would provide for enhanced punishment for identity theft and other violations of data privacy and security, require security standards for certain types of personal and account information, require certain disclosure and maintenance procedures for data brokers, and authorize the Attorney General and state attorneys general to bring civil actions against business entities for violations of the Act.

While supporting some aspects of proposed legislation, NAFCU has developed a list of items we would like to ultimately see addressed in any comprehensive data security bill:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card fraud be reduced. A reasonable and equitable way of addressing this concern would be to require merchants to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame. The entity that is best situated to mitigate the risk to sensitive data should be the liable party when a breach occurs.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no similar comprehensive

regulatory structure akin to GLBA that covers retailers, merchants, and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any business entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to by providing their personal information. NAFCU believes that this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant, but would provide an important benefit to the public at large.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the timely disclosure of identities of companies whose data systems have been violated, so consumers are aware of those that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and continue to store sensitive personal data in their easily breached systems.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised, personally identifiable information when associated accounts are involved.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the entity that has been breached. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information, but sustained a violation

regardless. The law is currently vague on this issue, and NAFCU therefore asks that this burden of proof be clarified in statute.

There are two motivating factors as to why those who collect and hold sensitive information do not do enough to protect it. First, the cost associated with the data breach often falls on others. Second, because others – for example a financial institution issuing the payment cards with new numbers – generally have to repair the problems caused by a data breach, consumers often incorrectly assume that these institutions were responsible for the breach. The first notification consumers often receive that their information may be compromised is often a call or letter from their credit union. By looking out for, and taking care of, their members, credit unions (and other financial institutions) can unintentionally suffer ill will from a member who finds out that their payment card from that institution has been re-issued. Thus the companies responsible for the data breach in the first place oftentimes do not suffer any loss of customer goodwill; at the same time consumer confidence in financial institutions, such as credit unions, may suffer. Furthermore, for a credit union such as AAFCU that serves a number of military members that may be deployed overseas, the impact on those members is magnified due to the longer postal time to get new cards to them.

While, the reputation risk to financial institutions may be difficult to solve with legislation, Congress should consider holding accountable those companies that are responsible for significant data breaches. There must be a strong incentive for businesses to properly protect consumer's financial data, otherwise, as evidenced by recent instances of payment card breaches,

the information may not be adequately protected and the credit union could end up being the one that pays.

Obviously, data breaches will continue to be a fact of life for any company that holds personal information. Unfortunately, no matter how quickly government and industry reacts, criminals will always find new and inventive ways around security measures. It is important that there be stiff penalties and full enforcement of the laws that prohibit and punish the actual criminals who take the action to commit these breaches by stealing, and often selling or using this compromised data. However, additional federal incentives to protect data are absolutely necessary. Any legislation that does not place the burden on responsible parties will ultimately prove toothless. Current data security standards established by payment card companies such as Visa and Mastercard prohibit storing sensitive data and even impose fines for those that do. However, either because the penalties are not harsh enough or the contracts aren't enforced, data ends up being stored improperly and breaches still end up occurring.

Finally, it should be noted that financial losses to credit unions are especially troubling, because unlike banks and other financial institutions, credit unions do not make profits for shareholders, do not issue stock, and aren't able to turn to capital markets for money to make up for data breach losses. All monies at a credit union must be raised through its members. Financial losses to the credit union are ultimately passed back to the member in the form of either reduced services, lower dividends on savings, higher interest rates on loans (either personal or business), or even decreased availability of loans.

Conclusion

In conclusion, NAFCU supports new measures to ensure industry takes adequate steps to protect consumers' sensitive financial data. The most efficient way to address the growing number of data breaches is to create a comprehensive regulatory scheme for those entities that currently have none. A safe harbor for financial institutions already in compliance with section 501 (b) of Title V of the GLBA should be included in any data security bill. Further, if more regulations are needed to address new concerns, it should be the functional regulators that are charged with promulgating new rules. Finally, merchants, retailers, data brokers or any other party that holds sensitive consumer information should be held financially accountable if it is responsible for a data breach.

Thank you again, Chairwoman Ellmers, Ranking Member Richmond, and members of the Subcommittee for the invitation to testify before you today. NAFCU appreciates the opportunity to weigh in on this important issue..