National Association of Federal Credit Unions
3138 10th Street North • Arlington, Virginia • 22201-2149
703-522-4770 • 800-336-4644 • 703-522-0594

B. Dan Berger
Executive Vice President
Government Affairs

June 20, 2011

The Honorable Tim Johnson
Chairman
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington DC 20510

The Honorable Richard Shelby
Ranking Member
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington DC 20510

Dear Chairman Johnson and Ranking Member Shelby:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federal credit unions, I am writing in conjunction with your Committee's hearing, "Cyber Security and Data Protection in the Financial Sector." We appreciate your attention to this significant issue.

The risk of a data security breach continues to be a serious problem for both consumers and businesses. Every time a consumer chooses to use a plastic card for payment at a register, they are unwillingly put at risk. Many are not aware that their financial identities may be stolen or that fraudulent charges could appear on their account, damaging their credit scores and reputations. These consumers trust that merchants will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, this is not always true.

As you may be aware, financial institutions, including credit unions, bear a significant burden as the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud related losses, many of which stem from a negligent retailer's failure to protect sensitive financial information or the illegal maintenance of such information in their systems.

In recent weeks, a number of Americans have once again turned to their credit unions and other financial institutions to resolve fraud related issues caused by the data breach at Michaels Stores, Inc. Because both debit cards and corresponding PINs were compromised, victims have seen money taken directly out of their checking accounts. Just last week, it was reported that law enforcement officials in Los Angeles believe hundreds of thousands of dollars fraudulently withdrawn from ATMs in California are related to the Michaels Stores data breach.

This demonstrates what we have been communicating to Congress all along; credit unions and other financial institutions, not retailers, are out front protecting consumers in picking up the pieces after a data breach occurs. It is the credit unions and other financial institutions that must notify their account holders, issue new cards, replenish stolen funds, change account numbers, and accommodate increased customer service demands that inevitably follow a major data breach. The negligent merchant who caused these expenses by failing to protect consumer data loses nothing and is often undisclosed to the consumer. Interchange fees have historically been one way in which the costs of such breaches were offset by merchants. However, last year's congressional action to limit debit interchange fees did not account for these costs, and thus will result in heavier burdens falling on financial institutions and consumers.

Furthermore, the ultimate cost of the Michaels Stores debit card data breach to financial institutions may not be fully calculated before the debit card interchange price-fixing caps go into effect on July 21, 2011; providing further evidence of the need for comprehensive data security legislation.

NAFCU is pleased to see the Committee begin considering the data security issue. As the Committee's work moves forward, NAFCU specifically recommends examination of the following issues for inclusion in any data security bill:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be requiring that merchants are held accountable for the costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information is safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for keeping consumers' personal information safe. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants, and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any business entity that is responsible for the storage of consumer data meet a set of standards similar to those imposed on financial institutions under the Gramm-Leach-Bliley Act.

- **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 the identities of companies and merchants whose data systems have been violated so consumers can be 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 merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems which, in many cases, can be easily breached.

- **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 merchant or retailer who incurred the breach. 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 current law is vague on this issue and therefore, NAFCU asks that this burden of proof be clarified in statute.

In addition to these recommendations, NAFCU would also like to note that there are critical homeland security considerations at stake when deliberating data safety issues. Weaknesses in the protection of consumer information can and has helped terrorist networks and organized crime groups fund their operations. NAFCU believes it is critical that these simple changes are enacted so as not to facilitate the financing of operations that threaten not only the financial stability, but also the livelihood of millions of Americans.

Thank you for your kind attention to this important matter. We appreciate the opportunity to voice our concerns, and look forward to working with you as the Committee examines this issue. Should you have any questions or requests for additional information, please do not hesitate to contact myself or NAFCU's Vice President of Legislative Affairs, Brad Thaler, at 703-842-2204.

Sincerely,

B. Dan Berger
Executive Vice President of Government Affairs

cc: Members of the Committee