NAFCU
**National Association of Federal Credit Unions**
3138 10th Street North • Arlington, Virginia • 22201-2149
703-522-4770 • 800-336-4644 • Fax 703-522-2734

**Fred R. Becker, Jr.**
*President and CEO*

June 1, 2011

The Honorable Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing and Trade
House Energy & Commerce Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable G.K. Butterfield
Ranking Member
Subcommittee on Commerce, Manufacturing and Trade
House Energy & Commerce Committee
U.S. House of Representatives
Washington, DC 20515

Dear Chair Bono Mack and Ranking Member Butterfield:

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 Subcommittee's hearing entitled "Sony and Epsilon: Lessons for Data Security Legislation." We appreciate your continued attention to this important issue.

As we have previously communicated, continued and ever-increasing data security breaches at retailers are a very serious problem for both consumers and businesses. Each year, millions of consumers are put at risk when they use plastic cards that their financial identifies may be stolen, fraudulent charges will appear on their account and their credit scores damaged. Financial institutions, including credit unions, also 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 the failure of retailers to protect sensitive financial information or the illegal maintenance of such information in their systems.

Unfortunately, in the few weeks since the Subcommittee's last hearing on data security, countless numbers of Americans are now turning to their credit unions and other financial institutions once again to resolve fraud related issues caused by a recent data breach at another major big box national retailer – Michaels Stores, Inc. Because both debit cards and corresponding PINs were compromised, victims have reportedly seen money taken directly out of their checking accounts, putting credit unions on the front line of combating fraud and protecting consumers.

Sadly, this demonstrates what we have been communicating to Congress for some time—that credit unions and other financial institutions, and not retailers, are the ones out front protecting consumers in picking up the pieces after a data breach occurs. This recent breach is a prime example of the role that debit interchange plays in ensuring the payments system operates smoothly and efficiently for consumers and financial institutions. Making the consumer "whole" comes with a cost such as replacing money pilfered from accounts, replacing compromised cards, setting up new accounts and heightened customer service demands that inevitably follow any major data breach, such as this. This cost, until now, has been made up by debit interchange. Unfortunately, the Federal Reserve's proposed price-cap rule that emerged from the debit interchange amendment in the *Dodd-Frank Act* did not factor in all of the costs associated with debit card fraud. Furthermore, the ultimate cost of this Michaels Stores debit card data breach to financial institutions may not be fully calculated before the debit card price caps go into effect on July 21, 2011, clearly demonstrating the need to delay the implementation of these new price caps and study the issue further so that the best decisions can be made on the interchange issue and data security.

It is with this in mind that we urge your support for H.R. 1081, the *Consumers Payment System Protection Act* introduced by Representatives Capito and Wasserman Schultz.

Furthermore, as the Subcommittee considers any data security legislation, NAFCU specifically recommends examination of the following issues:

- **Payment of Breach Costs by Breached Entities:** In cases of data breaches or fraud, it is the credit union that must notify its members, issue new cards, and change account numbers, all of which are time-consuming for staff and costly for the institution. Even where the merchant is at fault, it is still the financial institution that is responsible for making the consumer whole. While interchange fees have traditionally been a way in which the cost of such breaches could be offset, recent Congressional action under the *Dodd-Frank Wall Street Reform and Consumer Protection Act* will result in limits being imposed on this important source of business-to-business revenue. NAFCU therefore asks that credit union expenditures for breaches resulting from card use also be reduced. A reasonable and equitable means of addressing this concern would be to require merchants to be accountable for costs of data breaches that result from their own neglect.

- **National Standards for Safekeeping Information:** Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. 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 responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the Gramm-Leach-Bliley Act. It is critical that sensitive personal information be safeguarded at all stages of transmission.

- **Data Security Policy Disclosure:** One concern among many consumers is that they are unaware of the risks they are being 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 also believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of the names of companies and merchants whose data systems have been violated, so that consumers are aware of entities that may place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** Another concern that NAFCU believes is imperative to address is 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 such sensitive personal data in their systems, which can be breached easily.

- **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 also 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 of demonstrating 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.

In addition to these recommendations, NAFCU would also note that there are critical homeland security considerations at stake when deliberating data safety issues. Weaknesses in the protection of consumer information can and have helped terrorist networks and organized crime groups fund their operations. NAFCU believes it is critical that these simple changes be 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 address this issue and look forward to working with you as the Subcommittee examines this issue. Should you have any questions or need additional information, please do not hesitate to contact myself or NAFCU's Vice President of Legislative Affairs, Brad Thaler, at 703-842-2204.

Sincerely,

Fred R. Becker, Jr.
President and CEO

cc: Members of the Subcommittee