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

July 19, 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 mark-up of H.R. 2577, the *SAFE Act*. We appreciate your continued attention to this important 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 unwittingly 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 these 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.

While NAFCU is pleased to see the Subcommittee consider a data security bill, we would urge the Subcommittee to add a provision to Section 3 requiring timely notification of financial institutions whose accounts may have been impacted by the breach. Furthermore, as you consider the legislation, NAFCU specifically recommends addressing the following issues in any final 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 to require merchants to be accountable for 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 be safeguarded at all stages of transmission. 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.

- **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 disclosure of identities of companies and merchants 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 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 can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they have been 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 law is currently vague on this issue and NAFCU therefore asks that this burden of proof be clarified in statute.

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 Subcommittee tackles 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,

B. Dan Berger
Executive Vice President, Government Affairs

cc: Members of the Subcommittee