NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org

National Association of Federal Credit Unions | www.nafcu.org

February 4, 2015

The Honorable Jerry Moran
Chairman
Subcommittee on Consumer Protection,
Product Safety, Insurance & Data Security
Commerce, Science & Transportation Committee
U.S. Senate
Washington, D.C. 20510

The Honorable Richard Blumenthal
Ranking Member
Subcommittee on Consumer Protection,
Product Safety, Insurance & Data Security
Commerce, Science & Transportation Committee
U.S. Senate
Washington, D.C. 20510

Re: The Importance of Data Security to Our Nation's Credit Unions

Dear Chairman Moran and Ranking Member Blumenthal:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the interests of our nation's federal credit unions, I write to thank you for your efforts in taking steps to protect consumers from cyber and data security threats. NAFCU will closely monitor tomorrow's hearing, "Getting it Right on Data Breach and Notification Legislation in the 114th Congress." A chief concern of credit unions and their 100 million members continues to be data breaches at our nation's retailers exposing financial and personal data of millions of consumers.

As you know, consumers at risk in the wake of a data breach often rely on their credit union to help re-establish financial safety. In the process, credit unions suffer steep losses through the reissuance of cards, the charge-off of fraud, and the staff time it can take to respond to the magnitude of many of the breaches we have seen recently. Unfortunately, not all entities are held to a federal standard in protecting sensitive financial and personal information. While credit unions have been subject to federal standards on data security since the passage of *Gramm-Leach-Bliley Act* in 1999, the same cannot be said for our nation's retailers.

NAFCU member credit unions and their members have suffered greatly at the hands of negligent entities and have long sought legislation that would ensure retailers abide by a federal data security standard to better protect consumers. As your subcommittee looks at legislative solutions to address the data breach epidemic, we believe the following areas must be addressed:

- **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 entities 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 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 when they provide their personal information. NAFCU believes 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.

- **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.

- **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 the ones 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 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 nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

Thank you for your attention to this important matter. We look forward to tomorrow's hearing and working with the subcommittee as you move forward in addressing data security issues. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Director of Legislative Affairs Jillian Pevo at (703) 842- 2836.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee