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

March 12, 2013

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

**Re: Tomorrow's Cybersecurity Hearing**

Dear Chairman McCaul and Ranking Member Thompson:

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 regards to tomorrow's hearing on cybersecurity. As the Committee addresses this important issue, we urge you to not overlook the significance of financial data security.

The risk of a data 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 or the accounts attached to them for online payments, they are unwittingly put at risk. Many are not aware that their financial and personal identities could be stolen, or that fraudulent charges could appear on their account, damaging their credit scores and reputations. These consumers trust that entities collecting this type of information 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 entities failure to protect sensitive financial and personal information, or the illegal maintenance of such information in their systems. Moreover, as many identity thefts have been attributed to data breaches and identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to a minimum standard for protecting such data.

There have recently been several large-scale data breaches, such as the ones at Sony and Michael's Inc. The aftermath of these breaches demonstrates what we have been communicating to Congress all along; credit unions and other financial institutions, not retailers or other entities are out front protecting consumers in picking up the pieces after a data breach occurs. It is the credit union or other financial institution 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 entity that caused these expenses by failing to protect consumer data loses nothing, and is often undisclosed to the consumer.

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.

NAFCU is pleased to see the Committee begin to debate cybersecurity, and urge you to consider efforts to protect consumers from breaches that compromise their financial and personally identifiable information as part of this debate. The issue of data security is one of the priorities outlined in NAFCU's five-point plan for credit union regulatory relief, and recommend examination of the following issues for inclusion in any bill that seeks to address cybersecurity and data security issues:

- **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 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.

- **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 to 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 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 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 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 you examine this issue. Should you have any questions or need additional information, please do not hesitate to contact myself or NAFCU's Associate Director of Legislative Affairs, Chad Adams, at 703-842-2265 or cadams@nafcu.org.

Sincerely,

Brad Thaler
Vice President, Legislative Affairs

cc: Members of the Committee on Homeland Security