NAFCU

3138 10th Street North
Arlington, VA 22201-2149
P: 703.842.2234
F: 703.522.0594
chunt@nafcu.org

Carrie R. Hunt
Senior Vice President of Government Affairs
and General Counsel

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

February 3, 2015

The Honorable John Thune
Chairman
Committee on Commerce,
Science, and Transportation
United States Senate
Washington, D.C. 20510

The Honorable Bill Nelson
Ranking Member
Committee on Commerce
Science, and Transportation
United States Senate
Washington, D.C. 20510

Re: Congress Must Tackle Cybersecurity and Data Security Together

Dear Chairman Thune and Ranking Member Nelson:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federally chartered credit unions, I write today regarding tomorrow's hearing, *Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework.* Credit unions serve over 100 million members across the country and we appreciate your attention to this important matter.

NAFCU supports the strengthening of existing mechanisms in place to address cybersecurity issues such as the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). These organizations work closely with partners throughout the government creating unique information sharing relationships that allow threat information to be distributed in a timely manner. NAFCU also has worked with the National Institute of Standards and Technology (NIST) on the voluntary cybersecurity framework released in 2013 designed to help guide financial institutions of varying size and complexity relative to reducing cyber risks to critical infrastructure. While the NIST initiative with the framework is a good step, it was drafted with large institutions in mind. Smaller institutions such as credit unions need guidance that is tailored to their size and available resources.

In addition to addressing cybersecurity needs, NAFCU is hopeful that Congress will soon take legislative action to address ongoing data security breaches at our nation's retailers. Data security is an important part of the cybersecurity discussion and every time a consumer uses a plastic card for payment at a register or makes online payments from their accounts, they unwittingly put themselves at risk. Traditionally consumers have trusted that entities collecting this type of information will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, in the wake of several headline grabbing retailer breaches in recent months, this does not seem to be the case today.

With the increase of massive data security breaches at retailers, from the Target breach at the height of holiday shopping in 2013 impacting over 110 million consumer records to the recent

Home Depot breach impacting 56 million payment cards, Americans are becoming more aware and more concerned about data security and its impact. A Gallup poll from October 12-October 15, 2014, found that 69 percent of U.S. adults said they frequently or occasionally are concerned about having their credit card information stolen by hackers, while 27 percent of Americans say they or another household member had information from a credit card used at a store stolen in the last year. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

Financial institutions, including credit unions, have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act* and it is critical that any data security legislation include language to ensure they are not subject to any new onerous or duplicative regulations. However, retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, and they become victims of data breaches and data theft all too often. While these entities still get paid, financial institutions 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 entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum federal standards for protecting such data.

NAFCU believes data security is an important part of the cybersecurity debate. Accordingly, we urge Congress to come together in a bipartisan way and put forward legislative recommendations to hold retailers to the same strict standards of data security and breach notification that financial institutions must already adhere to. 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 committee looks at legislative solutions to address cyber and data security, 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.

On behalf of our nation's credit unions and their nearly 100 million members, we thank you for holding this important hearing. 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 Vice President of Legislative Affairs, Brad Thaler, at (703) 842-2204.

Sincerely,

Carrie R. Hunt
Senior Vice President of Government Affairs & General Counsel

cc: Members of the Senate Committee on Commerce, Science, and Transportation