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

December 1, 2014

The Honorable Harry Reid
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, D.C. 20510

The Honorable John Boehner
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

**Re: "Cyber Monday" and the Need for National Data Security Standards**

Dear Leader Reid, Leader McConnell, Speaker Boehner, and Leader Pelosi:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federal credit unions, I write today as consumers across the country make purchases online and participate in "Cyber Monday." According to the forecast released by the National Retail Federation yesterday, 126.9 million shoppers plan to shop online today and 133.7 million shoppers were in stores or online over the Thanksgiving weekend. Unfortunately, history tells us that the odds are that some of them will become victims of a data breach during this holiday shopping.

With the increase of massive data security breaches at retailers, from the Target breach at the height of holiday shopping last year 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 acceptable 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.

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.

As we first wrote to Congress in February of 2013, as part of NAFCU's five-point plan on regulatory relief, there is a need for data security to be addressed by lawmakers. Every time consumers choose to use plastic cards for payments at a register or make online payments from their accounts, they unwittingly put themselves at risk. Many are not aware that their financial and personal identities could be stolen or that fraudulent charges could appear on their accounts, in turn damaging their credit scores and reputations. 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.

While some argue for financial institutions to expedite the switch to "chip and PIN" technology, the reality is that it is no panacea for data security and preventing merchant data breaches. Many "chip and PIN" cards were compromised in the Target data breach because the terminals at the point of sale only accepted magnetic strip technology. "Chip and PIN" technology does not protect against online fraud, as the technology is designed to hinder in-person fraud and card duplication. While advances in technology like the move to chip-and-PIN may help prevent some data breaches, it is only treating a symptom. Besides, from what some in the retail industry have recently suggested, financial institutions switching to the new technology may not mean that retailers make the move with them. Tom Litchford, vice president of retail technologies at the National Retail Federation, told *The Wall Street Journal* earlier this year (March 26, 2014, "Retail Association: Card Security Costs Outweigh Benefits for Many") that CIOs must weigh whether the costs to upgrade their payment systems are greater than the financial costs associated with fraud and that many retailers would upgrade on their own pace, based on the return on investment.

NAFCU continues to recommend that Congress make the following priorities in any legislation and act on the following issues related to data security:

- **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.

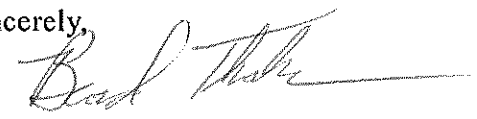
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that 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 98 million members, we thank you for your attention to this important matter. 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 United States Senate
Members of the United States House