NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.842.2215 | 800.336.4644
F: 703.522.2734
dberger@nafcu.org

B. Dan Berger
President & Chief Executive Officer

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

September 26, 2014

The Honorable Barack H. Obama
President of the United States
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Re: Holding Retailers Accountable For Data Breaches

Dear Mr. President:

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 as more news breaks that Home Depot confirmed a data security breach which led to the theft of customer credit and debit data. The Home Depot confirmed earlier this month that the breach started in April and affected as many as 56 million credit and debit cards. This is larger than the recent Target breach in terms of the number of cards affected. In fact there has been a number of data breaches announced in recent weeks, including at the United Parcel Service (UPS), Jimmy John's, Community Health Systems Inc., and at nationwide supermarket chain Supervalu. While the exact breadth and scope of these breaches are still being determined, one thing that is clear is that millions of Americans have had their personal information compromised.

These numerous breaches should lead to serious pause for the Administration, as the number of data breaches are broader and more frequent. These breaches come on the heels of the colossal Target breach, along with breaches at Smucker's, Sally Beauty, Neiman Marcus, Michaels, White Lodging, and countless other retailers in just the last year.

NAFCU calls on the White House to work with Congress to take legislative action to address data breaches that occur at the hands of retailers. As you know, there is no federal standard for merchants regarding the safekeeping of financial information or data breach notification efforts. This is having a huge impact on consumers everywhere and small financial institutions like credit unions struggle to make consumers whole in the wake of breaches they have no control over and didn't contribute to.

The Target breach of over 110 million records has been especially onerous on credit unions. Our member credit unions report that, on average, they have received hundreds of inquiries from their members seeking assistance due to the breach. NAFCU estimates that this particular breach could end up costing the credit union community nearly $30 million. This cost comes from fraud monitoring, reissuance of cards and actual losses from this breach. It does not even count the intangible cost of the staff time needed to handle all of the member service issues that stem from the breach. Unfortunately, credit unions will likely never recoup much of this cost, as there is no statutory requirement on merchants to be accountable for costs associated with breaches that result on their end.

These numbers echo what has historically happened to credit unions when a major retailer data breach occurs. A recent survey of NAFCU-member credit unions found that the 2006 data breach at TJ Maxx stores led to a median cost of $32,000 per institution, with only about 10% of those costs ever recovered on average.

As we first wrote to Congress in February of 2013 and again in August of 2014, 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.

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, <u>any entity that stores financial or personally identifiable information should be held to minimum standards for protecting such data.</u>

The need for legislation to bring additional entities, including merchants, handling sensitive consumer information into the federal regulatory rubric was underscored recently by estimates that one-third of the American public has been adversely impacted by the breaches disclosed over the last six months. While these breaches have drawn national attention, the reality is that data breaches are happening all the time, often on a smaller scale that does not make the nightly news. When taken together, these smaller breaches impact just as many consumers. According to the Identity Theft Resource Center, there were more than 600 reported data breaches in 2013 – a 30 percent increase over 2012. The business sector accounted for almost 82 percent of the breached records while the financial sector accounted for less than 2 percent of all breached records in 2013.

A recent Javelin Strategy & Research report (December, 2013) found that financial institutions are doing a much better job than retailers when it comes to credit card security. "Retailers, common targets for data breach crimes, scored the lowest in prevention and among the lowest overall," said Al Pascual, the senior analyst who co-authored the report. Furthermore, according to the Verizon 2013 Data Breach Investigation Report, a breakdown of incidents across various industries actually resulting from network intrusions, the retail industry was far and away the number one target, with nearly 22 percent of network intrusions occurring at retailers.

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. In addition, some in the retail

industry have recently suggested, a financial institution switching to the new technology will likely not mean that retailers make the move with them. Tom Litchford, vice president of retail technologies at the

National Retail Federation, recently told *The Wall Street Journal* (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 at their own pace, based on the return on investment.

As long as retailers are more concerned with their bottom line than protecting consumers, no one should expect their personal data to be protected. This is yet another fact highlighting the need for greater national data security standards as the way to truly help protect consumer financial information.

NAFCU urges the White House to work with Congress to 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. Again, we urge you to hold retailers to the same strict standards of data security and breach notification that financial institutions must adhere to. 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 Senior Vice President of Government Affairs/General Counsel, Carrie Hunt, at (703) 842-2234.

Sincerely,

B. Dan Berger
President and CEO

cc: Secretary Jack Lew, United States Department of Treasury