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**

January 13, 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

**Re: Enough is Enough; It's Time for Congressional Action on Data Security**

Dear Leader Reid and Leader McConnell:

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 to reiterate our call for Congress to take action on the issue of data security. With even more data breaches of retailers emerging, it is time for Congress to act and to hold hearings and craft legislation that will better protect consumers and ensure all entities handling their sensitive financial and personal information are held to the same high standards that financial institutions already are.

As you may have heard by now, last Friday Neiman Marcus Inc. joined the growing list of retailers reporting that the credit card information of its customers was stolen in a data security attack occurring over the holiday shopping season. While the extent of this incident and how many consumers have been impacted remains to be seen, it represents yet another data security breach and an additional source of worry for millions of Americans. Even more troublesome are news reports that additional retailers have been breached this holiday season, but have failed to report that information to the public in a timely manner so far.

Unfortunately, these developments come on the heels of emerging information in the massive Target Corporation data breach, with the company's recent revelation that 70 million consumers may have also had their personal information stolen, in addition to the previously reported 40 million card accounts that may have been compromised. This means that the true number of those impacted may top 100 million, not the 40 million originally reported. This astounding number should cause serious pause on Capitol Hill. The Target card data breach included the compromise of financial information such as credit and debit card numbers, expiration dates, and CVV security codes, as well as personal information such as e-mail and home addresses.

As we first wrote to you last February as part of NAFCU's five-point plan on regulatory relief, these incidents must 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 *Gramm-Leach-Bliley*. 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 standards for protecting such data.

Again, Neiman Marcus Inc. and the Target Corporation are just the latest in a string of large-scale data breaches impacting millions of American consumers. The aftermath of these and previous breaches demonstrate what we have been communicating to Congress all along: credit unions and other financial institutions – not retailers and other entities – are out in front protecting consumers, picking up the pieces after a data breach occurs. It is the credit union or other financial institution that must notify its account holders, issue new cards, replenish stolen funds, change account numbers and accommodate increased customer service demands that inevitably follow a major data breach. Unfortunately, too often the negligent entity that caused these expenses by failing to protect consumer data loses nothing and is often undisclosed to the consumer.

NAFCU reiterates its call on Congress to make the issue of data security a priority in 2014 by convening hearings on the data protection standards of merchants and what can be done to strengthen them and how retailers can better assist financial institutions when breaches occur. Furthermore, we recommend Congress take action to enact provisions to protect consumers from breaches that compromise their financial and personally identifiable information. Data security is a common-sense bipartisan issue that must be addressed.

With that in mind, NAFCU specifically recommends that Congress make it a priority to craft 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.

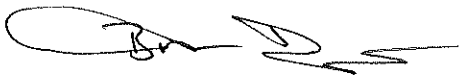
- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in 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 97 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 Vice President of Legislative Affairs, Brad Thaler, at (703) 842-2204.

Sincerely,



B. Dan Berger
President and CEO

cc: Members of the United States Senate