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 4, 2014

The Honorable Shelley Moore Capito
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

The Honorable Gregory Meeks
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

Re: Data Security: Examining Efforts to Protect Americans' Financial Information

Dear Chairman Capito and Ranking Member Meeks:

On behalf of the National Association of Federal Credit Unions, the only trade association exclusively representing the interests of our nation's federally chartered credit unions, I write today in advance of tomorrow's subcommittee hearing, "Data Security: Examining Efforts to Protect Americans' Financial Information." Data security is a chief priority of NAFCU member credit unions and the 97 million credit union members they serve. We appreciate the opportunity to share our concerns with you and look forward to the exploration of the impact of ongoing data breaches on consumers, as well as the community-based financial institutions that serve them.

Unfortunately, large national data breaches are becoming all too common. In just the last few months, consumers and credit unions have not only been affected by the recent Target Corporation breach, but also with additional national breaches at Neiman Marcus, Michaels and the White Lodging hotel management company. Tens of millions of Americans have been adversely impacted by these breaches. While these breaches draw national attention, many other "smaller" breaches are having just as much impact on the American consumer.

A January 2014, survey of NAFCU-member credit unions found that, on average, credit unions were notified over 100 times in 2013, of possible breaches of their members' financial information. That same survey found that nearly 80% of the time those notifications led to the credit union issuing a new plastic card to the member at their request because of the security breach, at an average cost of $5.00 to $15.00 per card.

The recent Target breach 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 recent Target 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 from the breach, with only about 10% of those costs ever recovered on average.

As we first wrote to Congress in February 2013, 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.

While some argue for financial institutions to expedite a switch to a "chip and pin" card, the reality is that chip and pin is no panacea for data security and preventing merchant data breaches. Many financial institutions that issue chip and pin cards had those cards stolen in the Target data breach, as the retailer only accepted magnetic stripe technology at the point of sale where the breach occurred. Furthermore, chip and pin cards can be compromised and used in online purchase fraud. This fact highlights the need for greater national data security standards as the way to truly help protect consumer financial information.

Again, recent breaches 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 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

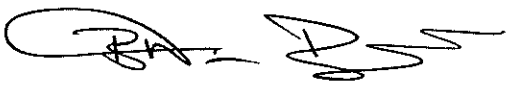
disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **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.

Again, on behalf of our nation's credit unions we thank you for your leadership on this issue and welcome the opportunity to work with you on legislation to strengthen data security standards for those who do not have such requirements now. 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 Subcommittee on Financial Institutions and Consumer Credit