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 12, 2015

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

Re: Thank You for Addressing Data Security and Ways to Enhance Consumers' Security

Dear Mr. President:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the interests of our nation's federal credit unions, I write today to thank you for your remarks at the Federal Trade Commission offices and for your Administration taking steps to protect consumers from cyber and data security threats. Data security continues to be a chief concern of our nation's credit unions and their 100 million members as breaches at some of our nation's largest retailers have exposed the financial and personal data of millions of consumers in recent months.

As your Administration builds on your Executive Order from last October and starts to craft your own legislative proposals, we hope retailers will be held to a *Gramm-Leach-Bliley Act* type of federal standard that credit unions are currently subject to. 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. We believe that more needs to be done to protect consumers and their financial institutions and that legislation is needed to address this problem.

It is with that in mind that NAFCU urges you to support the following credit union priorities in any data security legislation:

- **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 your attention to this important matter. We look forward to working with you on this important initiative. 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,

Thank you sir!

B. Dan Berger
President and CEO