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 16, 2015

The Honorable Fred Upton
Chairman
House Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Michael Burgess
Chairman
Subcommittee on Commerce,
Manufacturing and Trade
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing and trade
U.S. House of Representatives
Washington, D.C. 20515

Re: Discussion Draft of the *Data Security and Breach Notification Act of 2015*

Dear Chairman Upton, Ranking Member Pallone, Chairman Burgess and Ranking Member Schakowsky:

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 in advance of this week's Commerce, Manufacturing and Trade subcommittee hearing, "Discussion Draft of H.R.___, *Data Security and Breach Notification Act of 2015*." On behalf of NAFCU member credit unions and the 100 million credit union members across the country, we appreciate the subcommittee's attention to this very important matter. Still, NAFCU has concerns about the discussion draft and looks forward to working with you to address them as this issue moves forward.

While we appreciate the inclusion of a national standard for data security for retailers in the discussion draft, we believe the standard must be strengthened beyond "reasonableness." Just last week we wrote to Congress to bring your attention to a recently released *Verizon 2015 Payment Card Industry Compliance Report* which found that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. Massive data breaches at our nation's largest retailers continue to put millions of consumers at risk and have cost credit unions across the country millions of dollars in fraud related investigations and losses, card reissuance costs, and additional card monitoring. While a "reasonable" standard described in the discussion draft is a good first step, without inclusion of a robust and mandated rulemaking, little will be done to prevent data breaches and protect consumers.

Also noted in the *Verizon Report*, out of every data breach they studied over the past 10 years, not one single company was in compliance with the PCI standards at the time of the breach. This should cause serious pause among lawmakers as failing to meet these standards, exacerbated by the lack of a strong federal data safekeeping standard, leaves merchants, and therefore consumers, more vulnerable to breaches. If retailers cannot be trusted to comply with contractual obligations in an ongoing manner, nothing short of a national standard with the threat of monetary penalties for noncompliance will ensure that consumers are protected from identity theft and financial fraud. NAFCU believes that this level of data security cannot be achieved by the discussion draft in its current form.

Additionally, we believe that greater clarity of who is exempt from the definition of "covered entity" in the discussion draft needs to be provided. Credit unions are already covered by Federal data protection standards and notification laws and should not be subject to dual and inconsistent regulation. We appreciate that the discussion draft attempts to address this, but we believe that this language needs to be improved upon as we are concerned that some credit unions may fall under the "covered entity" definition as the language is currently drafted.

We also urge the inclusion of language to make those entities that fail to meet a data protection standard liable for any costs incurred from a breach of their systems. At the very least, the legislation needs to ensure that credit unions and others maintain a right to seek legal redress of any costs that they incur from a data breach.

We also note the breach notification provisions contained in the discussion draft. It is important for consumers whose personal data may have been compromised to be made aware of the risk so that they can take proactive steps to ensure that their personal information is not used in a fraudulent manner. Notification, however, is a reactive approach rather than a proactive one that will prevent breaches from happening in the first place. Notification standards without robust data security standards will not help consumers protect their personal information from a breach. Furthermore, we believe it is important to clarify in the bill that credit unions should have the ability to inform their members of a data breach at another party, including where the breach may have occurred.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. The difference, however, is that credit unions have developed and maintain robust internal protections to combat these attacks and are required by federal law and regulation to protect this information and notify consumers when a breach occurs that will put them at risk—no matter what size of the institution. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to $1 million per day for compliance violations. These extensive requirements and safeguards have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999 as part of the *Gramm-Leach-Bliley Act* (*GLBA*). In contrast, retailers are not covered by ***any*** federal laws or regulations that require them to protect the data and notify consumers when it is breached.

The ramifications for credit unions and their members have been monumental. A February 2015 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were $226,000 on average. Of their losses, respondents expect to recoup less than 0.5% which amounts to less than $100 on average. Despite the claims of some trade groups, the fact remains that our members are not recovering anything close to what they are spending to make their members whole after a merchant breach.

Ultimately, NAFCU believes that any comprehensive data security legislation must address:

- **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 *GLBA*.

- **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.

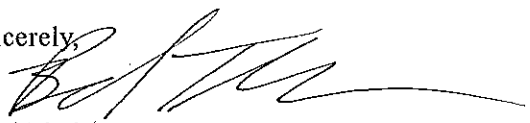
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that 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.

We urge the subcommittee and authors of the discussion draft to require a robust rulemaking for national data security standards in any final draft. Anything short of this will fail to provide consumers with the identity and financial protection that they want and deserve. We look forward to working with you and your staff on this data security legislation. 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 House Energy and Commerce Committee