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

May 18, 2015

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

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

Re: Tomorrow's Hearing: "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"

Dear Chairman Neugebauer and Ranking Member Clay:

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 regarding tomorrow's hearing entitled, "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats." We thank you for holding this important hearing and applaud your leadership on this matter.

As you know, the issues of cyber security and data security are intertwined. As Congress looks at cyber security issues, the need for greater data security standards for retailers must also be addressed. Consumers at risk in the wake of a data breach often rely on their credit union to help re-establish financial safety. In the process, credit unions suffer steep losses through the reissuance of cards, the charge-off of fraud, and the staff time it can take to respond to the magnitude of many of the breaches we have seen recently. Unfortunately, not all entities are held to a federal standard in protecting sensitive financial and personal information. While credit unions have been subject to federal standards on data security since the passage of *Gramm-Leach-Bliley Act* (GLBA) in 1999, the same cannot be said for our nation's retailers.

GLBA and its implementing regulations have successfully limited data breaches among financial institutions and this standard has a proven track record of success since its enactment. This record of success is why we believe any future requirements must recognize this existing national standard for financial institutions such as credit unions. One of the reasons for GLBA's success is the scalability rather than a one-size-fits-all approach. The best way to move forward and address data breaches is to create a comprehensive and similarly scalable regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

Consistent with Section 501 of the GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data to take appropriate steps to protect the security and confidentiality of the information.

The regulators published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business. This is a critical aspect of GLBA that allows flexibility and ensures the regulatory framework is workable for the largest and smallest in the financial services arena. As you consider cyber and data security measures, it should be noted that scalability is achievable and that it is misnomer when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying size businesses.

At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from

providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

- Background checks for employees with responsibilities for access to consumer information; and,
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies.
- Train staff to implement the credit union's information security program.
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. The difference, however, is that while retailers are not covered by *any* federal laws or regulations requiring data security or breach notification, credit unions must comply with the significant data security regulations outlined above, and undergo regular examinations to ensure that these rules are followed. Furthermore, a credit union faces potential fines of up to $1 million per day for compliance violations.

The ramifications of substandard data protections by retailers for credit unions and their members have been monumental. A February of 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.

Thank you for your attention to this important matter. We look forward to tomorrow's hearing and working with the committee as you move forward in addressing data and cyber security issues. 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 Subcommittee on Financial Institutions and Consumer Credit