



3138 10th Street North
Arlington, VA 22201-2149
P: 703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org

National Association of Federal Credit Unions | nafcu.org

April 19, 2016

The Honorable Steve Chabot
Chairman
Small Business Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Nydia Velázquez
Ranking Member
Small Business Committee
U.S. House of Representatives
Washington, D.C. 20515

Re: Cyber and Data Security

Dear Chairman Chabot and Ranking Member Velázquez:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today regarding tomorrow's hearing entitled, "Small Business and the Federal Government: How Cyber Attacks Threaten Both." A primary concern of credit unions and their 103 million members continues to be ensuring that our nation's retailers have the data and cyber security standards to protect consumers' information. We thank you for holding this important hearing and applaud your continued leadership on this matter.

NAFCU supports many of the ongoing efforts to strengthen the existing mechanisms in place to address cyber security issues, such as the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). These organizations work closely with partners throughout the government, creating unique information sharing relationships that allow threat information to be distributed in a timely manner. NAFCU also worked with the National Institute of Standards and Technology (NIST) on the voluntary cyber security framework released in 2013, designed to help guide financial institutions of varying size and complexity in reducing cyber risks to critical infrastructure.

Still, we believe more needs to be done on the data security front. Data security is an important part of the cyber security discussion and every time a consumer uses a plastic card for payment at a register or makes online payments from their accounts, they unwittingly put themselves at risk. Traditionally, consumers have trusted that entities collecting this type of information will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, in the wake of several headline grabbing retailer breaches in recent years, this does not seem to be the case today.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. The difference, however, is that financial institutions, including credit unions, have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act*. However, retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, even though they are often victimized in data breaches or by data thieves. While these entities still get paid, financial institutions bear a significant burden as

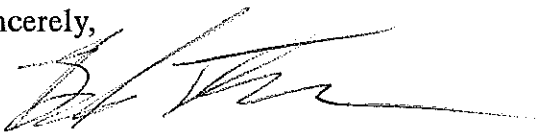
the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and 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 federal standards for protecting such data.

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.

NAFCU believes legislation pending before the House, H.R. 2205, the *Data Security Act of 2015*, would help address these concerns. This legislation would create a national standard of data security for all industries that handle sensitive information based on the standards in *Gramm-Leach-Bliley Act (GLBA)*, a key priority of NAFCU. It would also recognize that it is not productive to duplicate data protection and consumer notice requirements that are already in place for credit unions under GLBA. This legislation passed the House Financial Services Committee with a strong bipartisan vote last December. We urge committee members to support this legislative approach to this issue.

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 cyber and data 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 Senior Associate Director of Legislative Affairs, Chad Adams, at (703) 842- 2265.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the House Small Business Committee