



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

National Association of Federally-Insured Credit Unions

May 24, 2018

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing
And Urban Affairs
United States Senate
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, D.C. 20510

Re: Today's Hearing "Cybersecurity: Risks to the Financial Services Industry and Its Preparedness"

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write in conjunction with today's hearing, "Cybersecurity: Risks to the Financial Services Industry and Its Preparedness." Credit unions serve over 111 million members across the country and we appreciate your continued interest in fighting against cyber threats in the financial services sector.

Credit Unions are pleased to work with the National Credit Union Administration (NCUA) and the Federal Financial Institutions Examination Council (FFIEC) as regulatory partners in protecting credit unions and the financial system from cyber-attacks. While credit unions and other financial institutions have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA), including having federal regulators oversee and work with them on these standards, others such as retailers and merchants are not held to the same high standards of data security.

We recognize that a legislative solution is a complex issue, and thus have established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

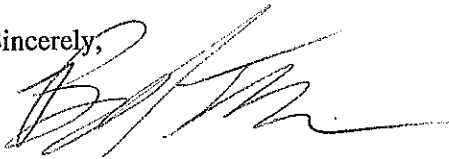
- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that 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 the GLBA, credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if those criteria are not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities 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 depository 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 those 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 negligent entity who incurred the breach.

Thank you for your continued interest in enhancing the security of the financial sector and for holding this important hearing. NAFCU urges Congress to come together in a bipartisan way and put forward legislative recommendations to protect financial institutions and ensure other entities who handle financial data are subject to strong national data security standards.

On behalf of our nation's credit unions and their 111 million members we thank you for your attention to this important matter. 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 me, or NAFCU's Associate Director of Legislative Affairs, Allyson Browning, at (703) 842-2836.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Senate Banking Committee