



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

March 6, 2019

The Honorable Rob Portman
Chairman
Permanent Subcommittee on Investigations
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

The Honorable Thomas R. Carper
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

Re: Tomorrow's Hearing on "Examining Private Sector Data Breaches"

Dear Chairman Portman and Ranking Member Carper:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with tomorrow's hearing entitled "Examining Private Sector Data Breaches." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 115 million consumers with personal and small business financial service products. NAFCU and our members welcome the Committee taking an important step by holding this hearing on data security.

Consumers and credit unions have suffered from large private sector data breaches, like the ones at Equifax and Marriott International. Credit unions suffer steep losses in re-establishing member safety after a data breach, often absorbing significant fraud-related losses. Credit unions and their members are victims in such breaches, as members turn to their credit union for answers and support. Furthermore, as credit unions are not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

NAFCU believes there is a need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements as depository institutions. While the *Gramm-Leach-Bliley Act* (GLBA) established a national data security standard for depository institutions over two decades ago, other entities who handle consumer financial data do not have such a national standard. Even though credit bureaus, such as Equifax, are governed by the GLBA's data security standards, they are not examined by a regulator for compliance with these standards in the same manner as depository institutions.

Although it may not help the millions of Americans that have been victimized by the breaches at Equifax and Marriott International, the time for Congress to act to prevent future breaches and harm to consumers is now. We recognize that a legislative solution to establish such a standard is a complex issue, and thus NAFCU has 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 from negligence on their end.
- **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.

NAFCU looks forward to working with you to establish a national data security standard that will ensure the security of consumer financial data. We are also pleased to work with those in industry to try to find common ground on a comprehensive proposal. We would urge the Subcommittee to work collaboratively with other interested Committees in the Senate to find a package that can advance and receive bipartisan support.

On behalf of our nation's credit unions and their more than 115 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information, please contact me or Alex Gleason, NAFCU's Associate Director of Legislative Affairs, at 703-842-2237 or agleason@nafcu.org.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Permanent Subcommittee on Investigations of the U.S. Senate Committee on Homeland Security and Governmental Affairs