



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**

October 5, 2021

The Honorable Maria Cantwell  
Chairwoman  
Committee on Commerce, Science,  
& Transportation  
United States Senate  
Washington, DC 20510

The Honorable Roger Wicker  
Ranking Member  
Committee on Commerce, Science,  
& Transportation  
United States Senate  
Washington, DC 20510

**Re: Tomorrow's Hearing, "Enhancing Data Security"**

Dear Chairwoman Cantwell and Ranking Member Wicker:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) ahead of tomorrow's hearing on "Enhancing Data Security." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 127 million consumers with personal and small business financial service products. NAFCU and our members welcome the Committee examining the important topic of data security.

As NAFCU has previously communicated to Congress, there is an urgent need for a national data security standard for entities that collect and store consumers' personal and financial information and are not already subject to the same stringent requirements as depository institutions. Unfortunately, retailers and fintechs are not held to the same data security expectations as depository institutions, which have faced rigorous cybersecurity exams for years under the *Gramm-Leach-Bliley Act (GLBA)*. Far too often these companies are the targets of data thieves because they do not have the same standards in place as financial institutions. Credit unions suffer steep losses in re-establishing member safety after a data breach and are often forced to absorb fraud-related losses in its wake. Credit unions and their members are the victims in such a breach, as members turn to their credit union for answers and support when such breaches occur. As credit unions are not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

NAFCU believes that negligent entities should be held financially liable for any losses that occur due to breaches on their end so that consumers are not left holding the bag. When a breach occurs, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts. Finally, any new rules or regulations to implement these recommendations should recognize credit unions' compliance with GLBA and not place any new burdens on them.

As we have shared with you before, we recognize that a legislative solution to data security 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 that 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 that 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.

The Honorable Maria Cantwell, The Honorable Roger Wicker

October 5, 2021

Page 3 of 3

- **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 that incurred the breach.

NAFCU thanks you for holding this important hearing and looks forward to working with the Committee and those in industry to address these concerns with consumer data security. On behalf of our nation's credit unions and their more than 127 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 Janelle Relfe, NAFCU's Associate Director of Legislative Affairs, at 703-842-2836 or [jrelfe@nafcu.org](mailto:jrelfe@nafcu.org).

Sincerely,



Brad Thaler

Vice President of Legislative Affairs

cc: Members of the Senate Committee on Commerce, Science, & Transportation