NAFCU
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

December 12, 2018

The Honorable Paul Ryan
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

Re: Recent Developments Highlight Continuing Need for Congress to Address Data Security

Dear Speaker Ryan and Leader Pelosi:

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 today to continue to urge Congress to take action to address data security issues given recent developments on the topic, including the report released this week by the House Oversight and Government Reform Committee on the Equifax Data Breach last year and the recent massive data breach at Marriott International.

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 that are not already subject to the same stringent requirements as depository institutions. While it may not help the millions of Americans that have been victimized by these recent breaches, the time for Congress to act is now to prevent future breaches and harm to consumers. We would urge your continued focus on this important topic and the need for addressing consumer data security issues in the remaining days of this Congress and in the new Congress.

While credit bureaus, such as Equifax, are governed by data security standards set forth by the *Gramm-Leach-Bliley Act* (GLBA), they are not examined by a regulator for compliance with these standards in the same manner as depository institutions. Additionally, as the recent House Oversight Committee report noted, the Equifax breach could have been prevented. NAFCU believes that when a breached entity knew or should have known about a threat, and fails to act to mitigate it, the negligent company must be held financially liable.

Credit unions suffer steep losses in re-establishing member safety after a data breach like the one at Equifax and are often forced to absorb fraud-related losses in its wake. Credit unions and their members are victims in this 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.

Negligent entities should be held financially liable for any losses that occurred due to breaches on their end so that consumers are not left holding the bag. When a breach occurs at a credit bureau, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts. Furthermore, compliance by credit bureaus with GLBA and

these notification requirements should be examined for, and enforced by, a federal regulator. 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.

NAFCU's Principles on Data Security

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 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.

We urge you to keep data security high on the Congressional agenda, both in the waning days of this Congress and when the 116th Congress convenes in January.

On behalf of our nation's credit unions and their more than 114 million members, we thank you for your attention to this important matter and stand ready to work with you. 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 U.S. House of Representatives