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

February 5, 2018

The Honorable Jerry Moran
Chairman
Subcommittee on Consumer Protection,
Product Safety, Insurance, and
Data Security
Committee on Commerce, Science,
& Transportation
United States Senate
Washington, D.C. 20510

The Honorable Richard Blumenthal
Ranking Member
Subcommittee on Consumer Protection,
Product Safety, Insurance, and
Data Security
Committee on Commerce, Science,
& Transportation
United States Senate
Washington, D.C. 20510

Re: Tomorrow's hearing, "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers"

Dear Chairman Moran and Ranking Member Blumenthal:

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 in conjunction with tomorrow's hearing on data security and the recent breach at Uber. We appreciate the Subcommittee's focus on this important topic. As NAFCU has previously communicated, the ever-increasing number of data breaches demonstrates the 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.

As you examine how to address data breaches, we would like to share a series of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security legislation. 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 *Gramm-Leach-Bliley Act* (GLBA), credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if that 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.

In the last Congress, NAFCU supported the bipartisan *Data Security Act*, S. 961, as a legislative approach that addressed a number of these principles. As you move forward with efforts to address data breaches, we would urge the Subcommittee to work collaboratively with the Senate Banking, Housing, and Urban Affairs Committee as well as the U.S. House of Representatives to advance comprehensive data security legislation in the year ahead.

On behalf of our nation's credit unions and their more than 110 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 Allyson Browning, NAFCU's Associate Director of Legislative Affairs, at 703-842-2836 or abrowning@nafcu.org.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee