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 15, 2019

The Honorable Michael Crapo
Chairman
Committee on Banking, Housing,
& Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing,
& Urban Affairs
United States Senate
Washington, DC 20510

Re: Your Request for Feedback on Data Privacy, Protection and Collection

Dear Chairman Crapo and Ranking Member Brown:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with your request for feedback on questions related to Data Privacy, Protection and Collection. 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 examining these important issues, and we have included our responses to your specific questions below.

1) **What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?**

Credit unions and their members are adversely impacted by continued data breaches at numerous merchants. The cost of dealing with these issues hinders the ability of credit unions to serve their members. While depository institutions have had a national standard on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA) over two decades ago, other entities who handle consumer financial data do not have such a national standard. That is why we believe that 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.

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.

Taken together, NAFCU believes these principles would establish a national standard to enhance consumer data protection and help ensure consumers are notified of data breaches in a timely and consistent manner.

2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies

(including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

Many consumers are unaware of the risks they are exposed to when they provide their personal information. As noted in our principles above, NAFCU believes this problem can be partially addressed by simply requiring merchants to post their data security/retention/sharing policies at the point of sale when they take sensitive financial data. The GLBA already places privacy policy disclosure requirements on financial institutions, and others who handle consumer data should face similar requirements. 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.

3) **What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?**

Consumers should know that their financial institutions, and the agencies that regulate them, have data security as a top priority. At NAFCU, we believe transparency of data use is one of the best tools to provide this confidence. This includes providing consumers with knowledge of what data is being collected from them, how it is being used and shared, data retention policies, and timely notification of any data breaches.

As outlined in the responses above, the time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Such a standard must recognize the existing protection standards that depository institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach. Once again, all "GLBA institutions," including credit bureaus, should be subjected to examinations by a regulatory body as depository institutions already are. Additionally, consumers whose personal and financial data has been compromised have a right to be notified in a timely manner. Depository institutions servicing the accounts should be made aware of any breach at a national credit bureau as soon as practicable so they can proactively monitor affected accounts, and any notification requirements should be enforced by a regulator. Congress needs to act to make this happen.

While some have said that voluntary industry standards should be the solution, the *Verizon 2015 Payment Card Industry Compliance Report* found that four out of every five global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. In fact, Verizon found that out of every data breach they studied over the 10-year study, <u>not one single company was in compliance with the PCI standards at the time of the breach</u>.

In addition, the report finds that the use of EMV cards ("chip cards") in other countries has not been a silver bullet solution to preventing fraudulent activity, but merely displaces it. The report shows that once EMV use increases, criminals shift their focus to card not present transactions,

such as online shopping. While some argued for the "chip card" solution, the reality is that it is not a panacea and does not replace a sound data security standard.

One basic but important concept to point out in regard to almost all data and cyber threats is that a breach may never come to fruition if an entity handling sensitive information limits the amount of data collected on the front end and is diligent in not storing sensitive personal and financial data in their systems. Enforcement of prohibitions on data retention cannot be over emphasized and it is a cost effective and commonsense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of cyber criminals.

4) What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

The foundation of America's national consumer credit system is the *Fair Credit Reporting Act*, enacted by Congress in 1970 to streamline credit reporting and provide consumers with protection from inaccurate and inappropriate disclosures of personal information by consumer reporting agencies. Credit bureaus collect and compile information about consumers' creditworthiness from financial institutions, public records, and other sources. Credit unions rely on this national credit system to assess lending risk, manage portfolios, detect fraud, acquire new members and grow those relationships. That is why we support a strong, robust and secure credit bureau system.

NAFCU and its member credit unions have also long advocated for the use of alternative models that more accurately capture creditworthy borrowers and permit them to access affordable credit. Credit unions have unique relationships with their members and should be permitted to choose the credit score model that best accommodates their members. NAFCU believes that improvements can be made to the current credit scoring system that allow credit unions to better serve their members without creating onerous new burdens.

The recent Equifax data breach also highlighted the need for addressing consumer data security issues at national credit bureaus and beyond. As NAFCU has long advocated to the Committee, 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 credit bureaus, such as Equifax, are governed by data security standards set forth by the GLBA, they are not examined by a regulator for compliance with these standards in the same manner as depository institutions. Additionally, the recent Equifax breach reportedly occurred via a "known" security vulnerability that software companies had issued a patch to fix several weeks prior. If Equifax had acted to remedy the vulnerability in a reasonable period of time, this breach may not have occurred. 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.

5) What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

NAFCU believes that certain changes to the *Fair Credit Reporting Act* would modernize the credit reporting system in a way that would benefit millions of consumers locked out of the current system.

One area to start would be the *Credit Access and Inclusion Act*. This legislation was introduced with bipartisan support in both chambers in the last Congress. The legislation is intended to allow low-income and minority Americans more access to credit and better credit options. The bill takes into account non-traditional payments, such as consumers' cell phone, rent, and utilities payments to be reported to the credit reporting agencies. The expectation is that this positive payment data will establish a positive credit score, and will in turn allow access to lower-cost loans, cheaper car payments, or mortgage qualification.

The ultimate goal is that with these additional means of establishing a credit score, consumers who previously had no access to credit will now have the opportunity to enjoy the economic rewards that come with positive credit scores. NAFCU believes this will have a positive impact on the overall financial health of individuals, as well as the American economy as a whole.

Thank you for the opportunity to share our thoughts on this important topic. We look forward to continuing to work with the Committee on this and other issues of importance to credit unions. 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

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Senate Committee on Banking, Housing, & Urban Affairs