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

March 25, 2019

The Honorable Raja Krishnamoorthi
Chairman
Subcommittee on Economic and Consumer Policy
Committee on Oversight and Reform
United States House of Representatives
Washington, DC 20515

The Honorable Michael Cloud
Ranking Member
Subcommittee on Economic and Consumer Policy
Committee on Oversight and Reform
United States House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing on "Improving Data Security at Consumer Reporting Agencies"

Dear Chairman Krishnamoorthi and Ranking Member Cloud:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with tomorrow's hearing entitled "Improving Data Security at Consumer Reporting Agencies." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 116 million consumers with personal and small business financial service products. We thank the Subcommittee for your focus on this important topic.

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.

The recent Equifax data breach has highlighted the need for addressing consumer data security issues at national credit bureaus and beyond. As NAFCU has long advocated, 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.

Unfortunately, data breaches have become a constant concern of the American people. Major data breaches now occur with an unacceptable level of regularity. A recent Gallup poll found that 69 percent of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers. These staggering survey results speak for themselves and should demonstrate the need for greater national attention to this issue.

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, 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.

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 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.

We thank you for examining this important topic today. NAFCU stands ready to work with you to address our concerns regarding the establishment of a national data security standard that will not only ensure the security of the credit bureau system, but also consumer financial data held by others, such as retailers.

On behalf of our nation's credit unions and their more than 116 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 Max Virkus, NAFCU's Associate Director of Legislative Affairs, at 703-842-2261 or mvirkus@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Economic and Consumer Policy