NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.842.2215 | 800.336.4644
f: 703.522.2734
dberger@nafcu.org | nafcu.org

B. Dan Berger
President & Chief Executive Officer

National Association of Federally-Insured Credit Unions

October 3, 2017

The Honorable Jeff Flake
Chairman
Subcommittee on Privacy,
Technology, and the Law
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy,
Technology, and the Law
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Re: The Equifax Data Breach

Dear Chairman Flake and Ranking Member Franken:

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 regarding the massive data breach that recently occurred at Equifax. The breach is another demonstration of the ongoing need for Congressional examination and action on the broader topic of data security. There is a need for a national data security standard for retailers and others who collect and store consumers' personal and financial information and are not subject to the same stringent requirements as depository institutions.

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.

Americans' sensitive financial and personally identifiable information will only be as safe as the weakest link in the security chain. While financial institutions, including credit unions, have been subject to federal standards on data security, and examination by regulators on these standards, since the passage of the *Gramm-Leach-Bliley Act* (GLBA), retailers and many other entities that handle sensitive personal financial data are not subject to these same standards. Consequently, they have become the vulnerable targets of choice for cybercriminals.

While credit rating agencies, such as Equifax, are governed by data security standards set forth by the *GLBA*, they are not examined by a regulator as depository institutions are. Additionally, the breach reportedly occurred through 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

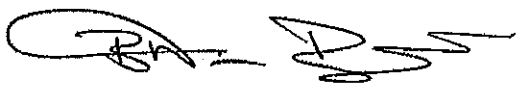
a reasonable period of time, this breach may not have occurred. When a breached entity knew or should have known about a threat, and fails to act to mitigate it, the negligent company must be held financially liable.

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.

Congress should implement national data security standards akin to *GLBA* for all entities that are not currently covered by the Act. Negligent entities should be held financially liable for any losses that occurred due to breaches on their end so that consumers aren't left holding the bag. Entities that are considered "GLBA institutions" should be regularly examined by a regulatory body, this includes national credit bureaus such as Equifax, which are not currently examined. Additionally, consumers whose personal and financial data has been compromised have a right to be notified. Depository institutions servicing the accounts should be made aware of a breach at national credit bureaus as soon as practicable so they can proactively monitor affected accounts, and any notification requirements should be enforced by a 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.

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 Brad Thaler NAFCU's Vice President of Legislative Affairs, at 703-842-2204 or bthaler@nafcu.org.

Sincerely,



B. Dan Berger
President and CEO

cc: Members of the Subcommittee on Privacy, Technology, and the Law