Credit Union National Association
CUNA

Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

May 7, 2019

The Honorable Jan Schakowsky
Chairwoman
Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers

On behalf of America's Credit Unions thank you for holding the hearing entitled "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security". The Credit Union National Association (CUNA) represents America's state and federal credit unions and the 115 million members that they serve.

We applaud the committee for taking up the critical issue of privacy and data security and we pledge to work with you to ensure that all Americans can expect that businesses are properly protecting their personal information. It should go without saying that any serious data privacy statute should include robust data security requirements that all who hold consumer data must follow. Unfortunately, as we have watched the debate over a federal data privacy standard develop, discussion of security requirements has been virtually nonexistent. Nevertheless, we do not see any way for a data privacy law to achieve its objectives without a strong security standard that is preemptive of state law and applies to all entities that hold or use consumer data. Simply put: Congress cannot provide consumer with data privacy without addressing data security.

Congress Should Treat Data Privacy as a National Security Issue
Since 2005, there have been more than 10,000 data breaches in the United States, compromising nearly 12 billion consumer records. These breaches are no longer just the work of lone domestic hackers. Time and time again, we learn that these breaches are being perpetrated by foreign governments, domestic organized crime syndicates and rogue international actors that use the data to help fund their illicit activity. We urge the Committee to treat this issue for what it is: a national security issue.

The Equifax data breach has resulted in the loss of 143 million consumers' records to criminals, which compromise the identities of these victims. Moreover, credit card numbers were also lost as part of Equifax's negligence, which have costs credit unions and their members significant losses from fraud and card replacement costs. Businesses that have lapses in data security should be subject to enforcement and should be required to pay damages to those harmed by their negligence.

Congress Should Fix the Weak Links in the System
If Congress is serious about protecting the privacy of consumers' data, then the guiding principle should focus on fixing the weak links that these criminals exploit. In this case, the weak link is that the entities that hold and use consumer data are not all subject to federal data security requirements. Financial institutions and health care providers have long been subject to federal laws that protect the use and security of consumers' and patients' information. These laws, the Gramm–Leach–Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act respectively, require financial institutions, including credit unions, and healthcare service

providers to have robust privacy and data security protections to protect and control the use of consumer and patients' data that they collect and house as necessary to provide *essential* services to Americans.

The privacy regulations required by the GLBA were originally promulgated by each financial institutions' regulator. This authority was transferred to the Consumer Financial Protection Bureau (CFPB) with the signing of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. The CFPB's privacy regulation requires that banks and credit unions provide an annual privacy notice to consumers, limits the sharing of information and allows consumers to opt-out of the limited sharing that is allowed. Credit unions and banks are also examined by federal and state regulators for compliance with privacy and data security laws.

The GLBA, although not perfect, has worked well and helped to solidify credit unions' and banks' long history of safeguarding information. We note that Equifax is also subject to GLBA data security standards; however, there is one key difference: Equifax is not examined for compliance with these data security requirements. Examination by a regulatory may be necessary to ensure privacy and data security compliance by entities that possess such a large amount of detailed records. It is long past time for all entities that hold or use consumer data to be subject to federal data security standards.

Congress Should Set a Strong Federal Standard that Preempts State Laws

With that vast amounts of data that businesses now collect with and without consumers' permission and/or knowledge, informed consent and even awareness of data collection and use becomes confusing for consumers. States are now stepping in to fill gaps to ensure consumers are protected when any business collects, uses or houses their information.[1] Although state privacy regulations can help consumers, they will also result in a patchwork of protections that will vary from state to state and likely result in many different privacy and data security requirements. A hodgepodge of state requirements will provide uneven protection for consumers and expensive compliance for businesses.

The best approach for consumers and business moving forward is for Congress to develop a strong privacy law that applies to all businesses and entities that collect, house or otherwise possess information. We urge you to take the best of state data security law, make it the federal standard and apply it to everyone. This will ensure efficiency for businesses and strong, consistent protections for consumers.

Conclusion

There is an urgent need for Congress to act to set a federal data privacy standard. The American consumer is under attack and current federal law leaves the door open for criminals, terrorist organizations and foreign governments to steal payment and other personally identifiable information to the benefit of their illicit activity. Taking a narrow view that this debate is about Facebook, Amazon and Google would be a grave mistake. There is no way for Congress to provide consumers with the data privacy they need without enacting robust data security standards that are preemptive of state law and apply to everyone.

On behalf of America's credit unions and their 115 million members, thank you for your consideration of our views on this important issue.

Sincerely,

Jim Nussle
President & CEO