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

February 26, 2019

Honorable Roger Wicker
Chairman
Committee on Commerce, Science & Transportation
United States Senate
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science & Transportation
United States Senate
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell:

On behalf of American's credit unions, I am writing to express our views ahead of the hearing titled "Policy Principles for a Federal Data Privacy Framework in the United States." The Credit Union National Association (CUNA) represents America's credit unions and their 115 million members.

Safeguarding consumers' money and personal information is the bedrock of the financial services industry and has been for a long time. In order to meet requirements of many different laws and regulations, financial services companies store and collect many different types of consumer information. The Gram-Leach-Bliley Act (GLBA) sets forth data security and privacy laws for credit unions and other financial intuitions. Other sectors are also subject to Federal requirements such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare providers.

HIPAA and GLBA have been in place for 20 years and reflect the importance of privacy and data security requirements for service businesses that must collect and store information in order to provide necessary services. Since these sector specific laws were passed by Congress, much has changed in the economy. There are many more businesses now that collect, aggregate, and sell Americans' most personal information; even traditional businesses like retailers have found value in collecting and analyzing their customers' data.

Since Americans' personal information has become so valuable in the aggregate to businesses and criminals worldwide, the time has come for new Federal protections regulating the use and security of data held by all businesses and entities. Europe's General Data Protection Regulation (GDPR) and California's California Consumer Privacy Act (CCPA) show that foreign governments and states are not willing to sit on the sidelines and neither should Congress. Action is required to ensure that all Americans can enjoy robust protection of their most important personal data from misuse and theft.

Credit unions have met with members of this committee to detail damage to credit unions and their members from data breaches. The current gaps in data protection and privacy laws hurt consumers and businesses as information is misused by criminals and other actors with malicious intent. Financial institutions are at the vanguard for misuse of stolen data. Although data security is a major issue for credit unions, we realize the problem is much bigger than the financial services industry with robust privacy and data security requirements for all industries becoming increasingly necessary.

The cornerstone of any new privacy requirements should be robust data security requirements for business and other entities that collect consumers' personal information. The current patchwork of laws is complex even at the Federal level. For example, federally regulated depository institutions are subject to data security requirements promulgated by each entity's prudential regulator and subject to privacy requirements promulgated by the Consumer Financial Protection Bureau (CFPB) even though GLBA is the implementing law for both. Companies such as Equifax follow the Federal Trade Commission's (FTC) Safeguards rule and the FTC further uses UDAAP

to enforce data security and privacy requirements for entities not subject to specific requirements. Layering additional state laws onto these rules creates complex challenges for compliance which is challenging for the largest of businesses and nearly impossible for smaller businesses.

Although GLBA has served the financial services industry well, Congress must work with the Administration and industry to finally address consumer data privacy in a meaningful way. To that end,

- Any new privacy law should cover both privacy and data security. There cannot be privacy of data without protection from loss due to breach or other types of theft.
- The law should cover all institutions, not just tech companies, credit-rating agencies, and other narrow sectors of the economy. Any company that collects, uses or shares personal data or information has the opportunity to misuse the data or lose the data through breach.
- Data security requirements should be based upon protection of data to prevent theft and misuse. Notification or disclosure after the fact are important but are not the stopping point for adequate protection. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals, so robust protection is paramount for any new requirements.
- A law should provide mechanisms to address the harms that result from privacy violations and security violations, including data breach. Increasingly courts are recognizing rights of action for individuals and companies (including credit unions). However, individuals and companies should be afforded a private right of action to hold those that violate the law accountable, and regulators should have the ability to take action against entities that violate the law.
- Any new law should preempt state requirements to simplify compliance and create equal expectation and protection for all consumers. Just like moving away from the sector specific approach, the goal should be to create a national standard for all to follow.

On behalf of America's credit unions, thank you for the opportunity to share our views.

Sincerely,

Jim Nussle
President & CEO