



WASHINGTON, D.C.
99 M Street SE
Suite 300
Washington, D.C. 20003-3799
Phone: 202-638-5777
Fax: 202-638-7734

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230
Attn: Privacy RFC

RE: Docket No. 180821780– 8780–01 - Developing the Administration’s Approach to Consumer Privacy

To Whom It May Concern:

The Credit Union National Association (CUNA) appreciates the opportunity to submit comments to the National Telecommunications and Information Administration (NTIA) on its Developing the Administration’s Approach to Consumer Privacy request for public comment. CUNA represents America’s credit unions and their 110 million members.

Safeguarding consumers’ money and personal information is the bedrock of the financial services industry. In order to adhere to the requirements of an array of different laws and regulations associated with making financial transactions, financial services institutions store and collect a wide range of consumer information. Due to a history of self-regulation, enhanced through strict government standards, credit unions and the rest of the financial services industry have built a strong culture dedicated to protecting consumers’ personal information.

Unfortunately, many industries do not possess this same level of dedication to protecting consumers’ personal information and are not subject to the strict government standards to which financial institutions must adhere. This differential results in wide gaps in data protection and privacy standards that hurt both consumers and their financial institutions when inevitable data breaches occur and criminals use personal information to commit fraud and other crimes. Stopping merchant data breaches, which result in the loss of consumer data to criminals through cyber-crimes, remains a top priority for credit unions as they bear significant financial responsibility for fraud committed due to theft of members’ personal account information.

The cornerstone of any new privacy requirement should be robust data security standards for businesses and other entities that collect and hold consumers’ personal information. The seven goals outlined in the request for comment are meaningless if the entity holding the information cannot safeguard it from theft by criminals or other bad actors. Specifically, the *security* goal would serve as a proper starting line for the NTIA when considering appropriate data security regulations.

CUNA's priorities for data security, which we ask the NTIA to seriously consider, include:

- A flexible, scalable standard equivalent to what is in the Gramm-Leach-Bliley Act (GLBA) for data protection;
- A GLBA equivalent notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators when there is a reasonable risk that a breach of unencrypted personal information exposes consumers to identity theft or other financial harm;
- Consistent, exclusive enforcement of the new data security and notification national standard by the Federal Trade Commission (FTC) and state Attorneys General; and
- Clear preemption of the existing patchwork of often conflicting and contradictory state laws for all entities that follow this national data security and notification standard.

We realize that the NTIA might not have authority to write rules that meet all of the above suggestions, but CUNA's data security principles are based on similar requirements which are in place for the financial services industry. Again, we think the first priority of any new privacy requirements should be bolstering data security requirements for those not subject to federal regulation. Criminal access needs to be quelled before we can have a full discussion on how to effectively provide additional protections to consumers.

We look forward to working with the NTIA and all other stakeholders on ways to increase protections of consumer information. Should you have any questions about CUNA's comments, please feel free to contact me at 202.508.6705.

Sincerely,

Lance Noggle

Senior Director of Advocacy for Payment and Cybersecurity and Senior Counsel