Credit Union National Association

Jim Nussle
President & CEO

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

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

March 1, 2023

The Honorable Gus Bilirakis
Chairman
Energy and Commerce Subcommittee
on Innovation, Data and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Energy and Commerce Subcommittee
on Innovation, Data and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of America's credit unions, I am writing about your hearing "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy." CUNA represents America's credit unions and their more than 130 million members.

Credit unions strongly support the enactment of a national data security and data privacy law that includes robust security standards that apply to all who collect or hold personal data and is preemptive of state laws. We firmly believe that there can be no data privacy until there is strong data security. Securing and protecting consumer data is important not only for their individual financial health but as a further safeguard against rogue international agents and interference by foreign governments.

Data privacy and data security are major concerns for Americans given the frequency of reports of misuse of personally identifiable information (PII) data by businesses and breaches by criminal actors, some of which are state sponsored. Since 2005, there have been more than 10,000 data breaches, exposing nearly 12 billion consumer records. These breaches have cost credit unions, banks, and the consumers they serve hundreds of millions of dollars, and they have compromised the consumers' privacy, jeopardizing their financial security.

Stringent information security and privacy practices have long been part of the financial services industries' business practices and are necessary as financial institutions are entrusted with consumers' personal information. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the Gramm Leach Bliley Act ("GLBA"). GLBA's protection requirements are strengthened by federal and state regulators' examinations for compliance with the GLBA's requirements and robust enforcement for violations. Several of these significant regulatory requirements and internal safeguards include:

- Federal Requirements to Protect Information: Title V of the GLBA and its implementing rules and regulations require credit unions to protect the security, integrity, and confidentiality of consumer information.

- Federal Requirements to Notify Consumers: Credit unions are required to notify their members whenever there is a data breach where the misuse of member information has occurred or where it is reasonably likely that misuse will occur.

- Strong Federal Oversight and Examination: Under their broad-based statutory supervisory and examination authority, the National Credit Union Administration (NCUA) and the Consumer Financial Protection Bureau (CFPB) regularly examine credit unions for compliance with data protection, privacy, and notice requirements.

- Strong Federal Sanction Authority: Under numerous provisions of federal law, credit unions are subject to substantial sanctions and monetary penalties for failure to comply with statutory and regulatory requirements.

While this extensive legal and regulatory examination and enforcement framework ensures that credit unions robustly protect consumers' personal financial information, this safety net only extends to financial institutions. As consumers' personal information is disseminated to third parties, those protections end and credit unions and their members are adversely impacted by the lax data security standards at other businesses. These loopholes must end and a comprehensive data security and privacy framework that covers all entities that that collect consumer information and is preemptive of state laws must be established and this standard must hold those who jeopardize that data accountable through enforcement.

With that in mind, we ask the committee to consider the following data security and privacy principles for any comprehensive framework:

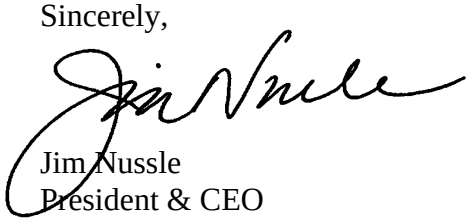
(1) **New Privacy and Data Security Laws Should Keep GLBA Intact:** Congress should leave financial services' robust data and privacy requirements in place. Financial services and the healthcare industry are subject to federal data privacy laws. The GLBA and the Health Insurance Portability and Accountability Act (HIPAA) have protected American's PII for over two decades and should be left in place as financial services and healthcare and their respective regulators have developed regulations, guidance, and procedures for compliance.
(2) **Data Privacy and Data Security Are Hand in Glove:** Any new privacy law should include both data privacy and data security standards. Simply put, data cannot be kept private unless it is also secured. Congress should enact robust data security standards to accompany and support data privacy standards.
(3) **Every Business Not Already Subject to Federal Law Should Follow the Same Rules**: The new law should cover all businesses, institutions, and organizations. Consumers will lose if Congress focuses only on tech companies, credit-rating agencies, and other narrow sectors of the economy because any company that collects, uses, or shares personal data or information can misuse the data or lose the data through breach.
(4) **There Should Be One Rule for the Road:** Any new law should preempt state requirements to simplify compliance and create equal expectation and protection for all consumers. We understand that some states have strong security and privacy requirements. Congress should carefully examine those requirements and take the best approaches from state law, as appropriate. A patchwork of state laws with a federal standard as a floor will only perpetuate a security system littered with weak links. The federal law should be the ceiling and the ceiling should be high. Just like moving away from the sector specific approach, the goal should be to create a strong national standard for all to follow.
(5) **Breach Disclosure and Consumer Notification Are Important, But These Requirements Alone Won't Enhance Security or Privacy**: Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals.

(6) **Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Regulatory Enforcement**: The 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 act against entities that violate the law.

(7) **Recognize This Issue For What It Is – A National Security Issue**: More and more, data breaches that expose consumer PII are perpetrated by foreign governments and other rogue international entities. The proceeds from these attacks are being used to fund illicit activity. The nature of these breaches alone calls for a strong federal response that ensures all involved in collecting, holding, and using PII do so with the security of the information of paramount concern. You simply cannot have data privacy unless there is data security.

On behalf of America's credit unions and their more than 130 million members, thank you for your consideration of our views and for holding this important hearing.

Sincerely,



Jim Nussle
President & CEO