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 28, 2023

The Honorable Patrick McHenry
Chairman
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

Dear Chairman McHenry and Ranking Member Waters,

On behalf of America's credit unions, I am writing regarding your committee's consideration of the Data Privacy Act of 2023. CUNA represents America's credit unions and their more than 130 million members.

We appreciate you and your staff's hard work to draft legislation to improve data security and privacy for financial institutions. Credit unions strongly support the enactment of a comprehensive 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.

We view this legislation as a mixed bag for credit unions. We support the goals of this legislation when considered as a substitute for the financial institution provisions in comprehensive data privacy legislation that the Energy and Commerce Committee may consider this year. However, we cannot support harmful provisions contained in this legislation, such as section § 501(c) on data usage, which would provide an extraordinary compliance burden on credit unions.

Provisions CUNA Supports

Stringent information security and privacy practices have long been part of credit unions' 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 regime that governs data practices for the financial services industry as set forth in the Gramm Leach Bliley Act (GLBA). The 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.

Any modernization of the GLBA must be predicated on the creation of this comprehensive data security and privacy standard that applies to all entities with access to the personally identifiable information (PII) of consumers. The breadth of security breaches and privacy violations of consumer data is currently unmatched—an epidemic that is exacerbated by the lack of a national standard. But this epidemic should not falsely be attributed to the credit unions, and other financial institutions, implementing strict protections and controls around consumers' data. The problem will not be solved by increasing the regulatory and financial burden on compliant institutions—all users and collectors of consumers' PII must be subject to the same standard. The GLBA, as written, provides tremendous protections for consumers that they are not receiving elsewhere and financial institutions have a strong commitment and interest in ensuring the continued protection of that data. American Data Privacy and Protection Act (ADPPA), passed out of the House Energy and Commerce Committee last Congress was a strong starting point for developing this standard as it imposed data security and privacy standards to all entities that collect consumer's personal information.

Securing and protecting consumer data is important not only for 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 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.

To alleviate these threats and concerns, credit unions support the following provisions outlined in the Data Privacy Act of 2023 that are in line with our principles on data security:

- Recognition of the burden on smaller financial institutions;
- Updated definition of a financial institution to include data aggregators;
- Preemption of conflicting state laws;
- Maintaining the status quo on enforcement through our prudential regulators.

Provision CUNA Opposes

CUNA has significant concerns about the inclusion of § 501(c) which can be interpreted as an "opt-in" for the use of all nonpublic personal information. Additionally, the § 502(e) exceptions apply to § 502 for collection and disclosure but not for *use*. As currently proposed, credit unions would have to obtain the affirmative consent of

their members for any *use* of data whenever they provide basic financial services. This creates an unwieldy, unsustainable system for credit unions that carefully manage existing uses of consumer data.

We ask that this section be removed entirely from the bill.

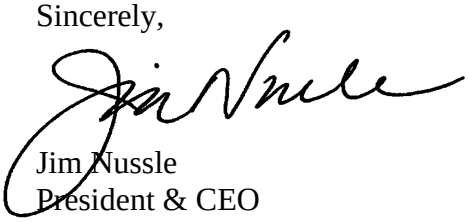
Conclusion

In conclusion, we oppose any amendments that may be offered that would change the following in the legislation:

- Remove a federal preemption;
- Add a Private Right of Action that does not include a safe harbor for financial institutions from liability for misuse of information when that information has been encrypted.

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

Sincerely,



Jim Nussle
President & CEO