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

June 22, 2022

The Honorable Janice D. Schakowsky
Chairwoman
Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Gus M. Bilirakis
Ranking Member
Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Schakowsky and Ranking Member Bilirakis,

On behalf of the Credit Union National Association (CUNA), I am writing regarding the mark-up of two bills before your Subcommittee: H.R. 8152, the American Data Privacy and Protection Act; and H.R. 3962, the Securing and Enabling Commerce Using Remote and Electronic Notarization Act of 2021. CUNA represents America's credit unions and their more than 130 million members.

H.R. 8152, the American Data Privacy and Protection Act

We appreciate the Committee bringing data security and privacy to the forefront. 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. With that in mind, credit unions strongly support the approach of the bicameral, bipartisan proposal that would cover all entities that collect consumer information and hold those who jeopardize that data accountable through regulatory enforcement.

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.

Although protecting members' data is of paramount importance to credit unions, credit unions and their members are adversely impacted by lax data security standards at other businesses. For example, CUNA members have reported a massive increase in fraud against state unemployment insurance programs. These reports have been

confirmed by the United States Secret Service. The fraud appears to be mainly coming from an international fraud ring that has the capacity to exploit many states' unemployment programs.

According to the Secret Service, the criminals are likely in possession of a vast amount of PII, which they are using to apply for unemployment insurance. It is almost certain that this PII was stolen in a data breach, or many data breaches, and it is now being used to exploit state unemployment insurance programs. This is clearly an example of how the multiple data breaches where PII has been stolen are causing harm to Americans and costing everyone money.

With that in mind, credit unions applaud the American Data Privacy and Protection Act's agreement with our data security and privacy principles as outlined in previous communications to the Committee:

New Privacy and Data Security Laws Should Keep GLBA Intact: We appreciate the acknowledgement of the efficacy of the GLBA standard and the protection and security it has provided to consumer data over the last two decades. The rules and regulations surrounding GLBA have been developed to respond to not only the needs of consumers but also to the size and resources of the financial institution. The requirements contained in this bill are especially onerous for institutions already complying with a strong data security and privacy framework. Compounding the regulatory burden on financial institutions, especially small institutions, would be especially onerous. We ask that the "related requirements" language of § 404 be removed and compliance with the strong security and privacy standards of GLBA and its implementing regulations be deemed compliant with the American Data Privacy and Protection Act.

Data Privacy and Data Security Are Hand in Glove: We are extremely supportive of the bill's comprehensive data privacy and data security framework. Credit unions feel strongly that data cannot be kept private unless it is also secured.

Every Business Not Already Subject to Federal Law Should Follow the Same Rules: The broad inclusion of all entities under Federal Trade Commission (FTC) jurisdiction, nonprofits, and telecommunications common carriers is vital to the protection of consumers because any company that collects, uses, or shares personal data or information can misuse the data or lose the data through breach. Credit unions strongly support this broad inclusion of entities.

There Should Be One Rule for the Road: The national standard established by this bill is crucial to ensuring data privacy and security, and credit unions champion this approach. The current patchwork of state laws perpetuates a security system littered with weak links and leaves entities and consumers on unequal footing in protecting data. While we recognize the bill's intent to preserve existing laws and regulations unrelated to the data security and privacy aims of this legislation, we do have concerns about potential loopholes in the preemption coverage of § 404(b)(2). The exclusion of laws governing the privacy rights of employees (§ 404(b)(2)(C)) as well as the exclusion of laws addressing "banking records, financial records, tax records, Social Security numbers, credit cards…" (§ 404(b)(2)(J)) provides for loopholes that states can exploit to disrupt the national standard established by this bill.

Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Regulatory Enforcement: We applaud the enforcement measures created in this legislation, and their ability to address the harms that result from privacy and security violations. Particularly the treatment of rights of action and the provision of a 45-day cure period for potential violations of the bill. We ask that the 45-day cure period be extended to cases brought by the FTC and state attorneys general. There will be a learning curve for implementation of this comprehensive national standard, and unintentional violations may occur. Allowing entities to cure these violations in good faith will aid compliance with this Act.

Additionally, we would like to express concern for the feasibility and financial burden of § 301's requirement that all covered entities designate a privacy officer and data security officer. There is currently a shortage of qualified employees in the data security and privacy space, and the addition of covered entities filling these roles would quickly exhaust the system. While we appreciate that small institutions would be exempted from this provision, the

shortage of available applicants will quickly drive up the market rate for these positions, pricing out institutions and requiring vital resources to be shifted from serving their communities to funding these roles. We recognize the importance of establishing the infrastructure within entities to ensure compliance with the provisions of this Act; however, that implementation must be feasible.

H.R. 3962, the Securing and Enabling Commerce Using Remote and Electronic Notarization Act of 2021

CUNA supports H.R. 3962, the Securing and Enabling Commerce Using Remote and Electronic Notarization Act, which would authorize the use of remote online notarization and create national standards and protections for its use.

Financial transactions are complicated and rely on the trust of both parties. Notarization requirements help ensure that these transactions are properly executed and validate the individuals presenting themselves as parties to the transaction. While several federal regulations require documents to be notarized, notary laws and regulations are generally governed at the state level.

The COVID-19 pandemic complicated person-to-person contact and made it difficult, if not impossible in some cases, to secure in-person notary services. Some states have remote notarization laws in effect; other states' governors issued temporary executive orders permitting remote notarization. However, given the fact that the pandemic has affected every state and county in the country and that many of the notary requirements emanate from Federal law, CUNA strongly believes it would be in the interest of public policy to have a federal law permitting remote online notarization.

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

Sincerely,

Jim Nussle
President & CEO