



**America's
Credit Unions**

Jim Nussle

President & CEO
202-508-6745

jnussle@americascreditunions.org

99 M Street SE
Suite 300

Washington, DC 20003

May 8, 2024

The Honorable John Hickenlooper
Chairman
Committee on Commerce, Science,
& Transportation
Subcommittee on Consumer Protection,
Product Safety, and Data Security
United States Senate
Washington, DC 20510

The Honorable Marsha Blackburn
Ranking Member
Committee on Commerce, Science,
& Transportation
Subcommittee on Consumer Protection,
Product Safety, and Data Security
United States Senate
Washington, DC 20510

Re: Today's Hearing: "Strengthening Data Security to Protect Consumers"

Dear Chairman Hickenlooper and Ranking Member Blackburn:

On behalf of America's Credit Unions, I am writing regarding today's hearing, "Strengthening Data Security to Protect Consumers." America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their nearly 140 million members nationwide.

Credit unions strongly support the idea of a national data security and data privacy regime 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.

Stringent information security and privacy practices have long been a part of the financial services industries' business practices and are necessary as financial services 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). The GLBA's data protection requirements are strengthened by federal and state regulators' examination and supervisory authority, which ensures compliance and permits robust enforcement for violations.

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 18,000 data breaches exposing billions of consumer records. These breaches have cost credit unions, banks, and the consumers they serve millions of dollars, and have compromised consumers' privacy, jeopardizing their financial security.

Mitigating losses from merchant data breaches remains a top credit union priority. Data breaches that expose card information and consumers' PII, as with the 2017 Equifax data breach,

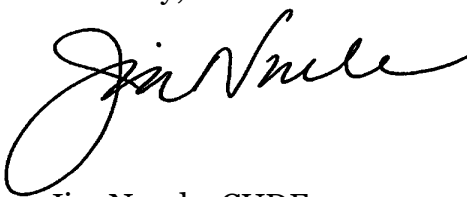
cost credit unions and their member-owners enormous sums of money. Additionally, this breach gave criminals copious amounts of personal information which could be used to directly defraud credit unions and other financial institutions. Even though financial institutions have an affirmative duty to make consumers whole for losses incurred from data breaches resulting in fraud on their accounts, the repercussions for both the financial institutions and the consumer are substantial.

Losses to credit unions from merchant data breaches impact credit union members in multiple ways. Even though credit unions bear the direct financial losses of fraud resulting from a merchant data breach, members also bear a cost as the owners of credit unions. Every credit union member is an equal owner who shares in the success of a credit union by receiving lower interest rates on loans, higher interest rates on deposit products, and lower fees. Due to credit unions' ownership structure, any loss from a data breach impacts members as their benefits are directly decreased by such losses. These losses can be exacerbated by credit unions' field of membership requirements, which can create geographic or industry-specific concentrations of members, leading to a more impactful data breach.

There are three key tenets that credit unions believe must be addressed in any new national data security and privacy law: a recognition of GLBA standards in place for financial institutions and a strong exemption from new burdensome requirements, a strong federal preemption from the myriad state laws for those in compliance with national privacy and GLBA standards, and protection from frivolous lawsuits created by a private right of action.

On behalf of America's Credit Unions and the nearly 140 million credit union members, thank you for holding this hearing and the opportunity to share our views. We look forward to continuing to work with you to create an environment where credit unions can thrive.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Nussle". The signature is fluid and cursive, with a large loop at the end.

Jim Nussle, CUDE
President & CEO

cc: Members of the Subcommittee on Consumer Protection, Product Safety, and Data Security