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

July 27, 2018

The Honorable Bob Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Dear Chairman Latta:

On behalf of America's credit unions, thank you for the opportunity to participate in discussions and consider our data security concerns. The Credit Union National Association (CUNA) represents America's credit unions and their 110 million members.

Mitigating losses from merchant data breaches remains a top credit union priority. Data breaches that expose card information and consumers' personally identifiable information, such as what happened with the 2017 Equifax data breach, cost credit unions and their member owners enormous sums of money and, in the case of Equifax, give criminals much personal information which can be used to directly defraud credit unions and other financial institutions. Even though financial institutions can and do make consumers whole for losses incurred from data breaches resulting in fraud on their accounts, time to fix problems and other risks from identity theft cannot as easily be fixed.

Losses to credit unions from merchant data breaches impact credit union members in multiple ways. Even though credit unions bear the direct financial losses from fraud resulting from a merchant data breach, members bear a cost as owners of credit unions because credit unions are member-owned organizations. Technically members are shareholders but in the cooperative sense, which means that 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 to a credit union from a data breach impacts members directly as their member benefits are directly decreased by losses from the breaches. These losses can be exasperated by credit unions membership requirements that can create concentrations of memberships and lead to a more impactful data breach.

CUNA favors data security legislation that places liability on a business that loses consumer information through a data breach and creates a mechanism for those harmed by the breach to recover losses from the breached entity. Although we believe breached entities should be responsible to others harmed from the breach, we believe Congress should consider how a member of a member-owned financial institution is harmed in multiples ways by a data breach. Absent

specific liability requirements, CUNA would not support legislation that diminishes a credit unions ability to recover through common law or other state provisions.[1]

While considering a broad data breach law, this Committee should look to small financial institutions' experience with the Gramm-Leach-Bliley Act (GLBA) data security standards. Financial institutions range in size from banks with over $2 trillion in assets to credit unions with less than $1 million in assets and not even a single full-time employee. All financial intuitions are subject to GLBA data security requirements and examined by regulators. Small credit unions meet GLBA standards and are examined by regulators for compliance. This experience with GLBA requirements demonstrates that even the smallest merchant or business can meet reasonable data security requirements based on risk, which is not necessarily tied to the size of a merchant but more to the number of records that could be lost.

CUNA priorities other than liability are highlighted in another letter signed by our organization and other financial trade associations. We are also including them here:

- A flexible, scalable standard equivalent to what is in the 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.
- 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.

Any data security legislation enacted by Congress must meet the requirements in this letter or it will fail to provide adequate protection to consumer and others harmed by data breaches. We look forward to continuing our work with Congress to provide additional recommendations. On behalf of America's credit unions and their 110 million members, thank you for your consideration.

Best regards,

Jim Nussle
President & CEO

[1] CUNA and member credit unions have filed data breach actions against Target, Home Depot, Wendy's and Equifax for harm caused to credit unions by these data breaches. Credit unions have received substantial settlements from Target and Home depot with litigation against Wendy's and Equifax ongoing.