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 16, 2020

The Honorable Emanuel Cleaver
Chairman
Subcommittee on National Security,
International Development and Monetary Policy
Committee on Financial Services
Washington, DC 20515

The Honorable French Hill
Ranking Member
Subcommittee on National Security,
International Development and Monetary Policy
Committee on Financial Services
Washington, DC 20515

Dear Chairman Cleaver and Ranking Member Hill,

On behalf of American's credit unions, I am writing to express our views ahead of the hearing titled "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic." The Credit Union National Association (CUNA) represents America's credit unions and their 115 million members.

We appreciate the Committee bringing cyber and data security and privacy to the forefront and we fully supports the Internet Fraud Prevention Act, which would require the Federal Reserve, Federal Trade Commission, and FBI to study and report on Business Email Compromise Scams and require the Federal Financial Institutions Examination Council to include Business Email Compromise Scams in its Bank Secrecy Act and Anti-Money Laundering (BSA/AML) exam procedures.

This effort could not be timelier. Nefarious actors are becoming more and more savvy, recruiting unsuspecting money mules – individuals who unknowingly transfer money acquired illegally in person, through a courier service, or electronically, on behalf of others. And, since the beginning of the pandemic, instances of reported cyber-attack have increased. Several of our member credit unions have reported attempts disguised as information from international organizations on COVID-19, as well as emails with links to make donations to various causes in support of phony COVID-related charities.

We have been advising our members to prepare for increased cyberattacks related to COVID-19 and have been encouraging the use of Virtual Private Networks (VPN) in order to mitigate undue risk while working remotely. But more clearly needs to be done. That is why we appreciate the subcommittee's consideration of Representative Gabbard's legislation, which would require Federal Regulators, including the National Credit Union Administration, to issue guidance encouraging financial institutions to educate their members and customers at the signs of money mule scams.

Credit unions' mission has always been to serve the underserved and we believe it is paramount that we assist and protect the most vulnerable during the pandemic. Financial exploitation is one of the most common and pernicious forms of elder abuse. CUNA strongly supports efforts to help protect seniors from financial exploitation and to empower seniors to make responsible decisions regarding their financial lives. CUNA long supported and was pleased to see enacted, the Senior$afe Act, which provides limited immunity for properly trained financial employees who disclose concerns about financial exploitation of senior citizens to the appropriate authorities. As such, CUNA supports the Senior Investor Pandemic and Fraud Protection Act, which would authorize grants to protect seniors and other vulnerable populations from misleading and fraudulent marketing or sales practices related to COVID–19.

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 as 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.

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 and example of how the multiple data breaches where PII has been stolen are causing harm to Americans and costing everyone money.

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. But it is not enough. It is long past time for Congress to enact a meaningful data security and privacy legislation that sets a nationwide standard and applies to businesses and financial institutions alike.

With that in mind, credit unions call on the Committee and Congress to follow the principles outlined below for Federal privacy and data security legislation:

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.

Everyone 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.

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.

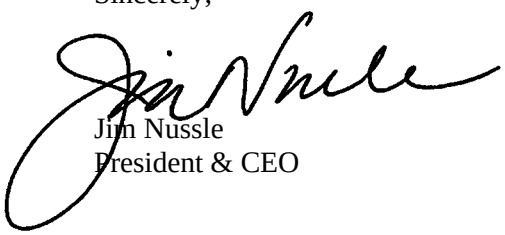
Breach Disclosure and Consumer Notification Are Important, But These Requirements Alone Won't Enhance Security or Privacy:
Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals.

Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Private Right of Action and 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.

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 115 million members, thank you for the opportunity to share our views on this important issue.

Sincerely,



Jim Nussle
President & CEO