

March 17, 2015

The Honorable Michael C. Burgess
Chairman
Subcommittee on Commerce,
Manufacturing and Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce
Manufacturing and Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

On behalf of the Credit Union National Association, I am writing to thank you for holding a hearing entitled “Discussion Draft of H.R. _____, Data security and Breach Notification Act of 2015”. CUNA is the largest credit union advocacy organization in the United States, representing nearly 90% of America’s 6,300 state and federally chartered credit unions and their 102 million members.

Credit unions are subject to high data protection standards under the *Gramm-Leach-Bliley Act*, and they take their responsibility to protect their members’ data seriously. Unfortunately, there is a weak link in the payments system that leaves consumers’ financial data vulnerable to theft by domestic and international wrongdoers. The weak link is the absence of Federal data security standards for the merchants that accept payment cards.

There have been several very high profile merchant data breaches in the last few years, notably the breaches at Target in 2013 and Home Depot in 2014. Millions of credit union members were affected by these two breaches, which ultimately cost credit unions – and by extension their members – nearly \$100 million. Despite the recovery efforts of payment card networks, no credit union has received a dime from the merchants whose security failure allowed the breach. Credit unions and their members are left on the hook.

These two breaches made headlines, but merchant data breach is a chronic issue. The endless string of breaches demonstrates clearly that those who accept payment cards need to be subject to the same Federal data standards as those who issue the cards.

It is important to recognize that the costs of a merchant data breach scenario on a small financial institution will be relatively greater than the costs of the same breach on large financial intuitions. For example, credit unions do not enjoy the economies of scale that national megabanks do. Therefore, the cost of everything, from replacing a debit card to monitoring suspicious activities, is greater.

The Honorable Michael C. Burgess
The Honorable Jan Schakowsky
March 16, 2015
Page Two

Credit unions join with our colleagues in the banking industry to call on Congress to enact meaningful data security legislation that incorporates the following principles:

- Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security regime, applicable to any party with access to important consumer financial information.
- Banks and credit unions are already subject to robust data protection and notification standards. These *Gramm-Leach-Bliley Act* requirements must be recognized.
- Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification standards.
- In the event of a breach, the public should be informed where it occurred as soon as reasonably possible to allow consumers to protect themselves from fraud. Banks and credit unions, which often have the most direct relationship with affected consumers, should be able to inform their customers and members about the breach, including the entity at which the breach occurred.
- Too often, banks and credit unions bear a disproportionate burden in covering the costs of breaches occurring beyond their premises. All parties must share in protecting consumers. Therefore, the costs of a data breach should ultimately be borne by the entity that incurs the breach.

There are a number of Congressional committees exploring remedies to merchant data breaches. Given the very direct and detrimental impact these breaches have on credit unions and banks, we have asked the House Financial Services Committee to take a leadership role in this effort. We understand and appreciate that the staff of the Energy and Commerce Committee and the staff of the House Financial Services Committee have recently discussed these matters together.

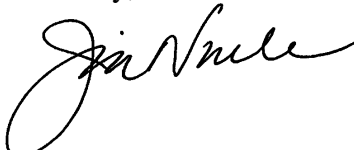
In addition to incorporating the principles outlined above into the legislation you are considering, we would like to bring to your attention a technical issue that we hope you will correct. We appreciate that you have exempted from the definition of covered entity certain financial institutions as defined under Section 5(a)(2) of the Federal Trade Commission Act. While this definition would exclude from the definition of covered entity all federally chartered credit unions, it does not exclude state chartered credit unions. That

The Honorable Michael C. Burgess
The Honorable Jan Schakowsky
March 16, 2015
Page Three

is why we suggest adding to Section 5(4)(B) on page 19 the following: “(iii) a depository institution as defined in section 19(b)(1)(A) of the Federal Reserve Act.” This ensures that state chartered credit unions are included in the exemption of covered entities.

On behalf of America’s credit unions and their 102 million members, thank you for considering our views on this very important topic for America’s consumers, which we are proud to serve as their financial institutions – we must all share responsibility in protecting consumer data.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Nussle". The signature is fluid and cursive, with a large initial "J" and "N".

Jim Nussle
President & CEO