



Credit Union National Association

cuna.org

**BILL CHENEY**  
President & CEO

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | **PHONE:** 202-508-6745 | **FAX:** 202-638-3389

September 14, 2011

The Honorable Patrick Leahy  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

The Honorable Charles Grassley  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

On behalf of the Credit Union National Association, I am writing regarding tomorrow's scheduled markup of legislation related to data security legislation (S. 1151 and S. 1408). CUNA is the largest credit union advocacy organization in the United States, representing nearly 90% of America's 7,600 state and federally chartered credit unions and their 93 million members.

S. 1151 establishes national standards for data security and data breach notification. S. 1408 would establish a data breach notification standard similar to the requirements of S. 1151. We are concerned that provisions of these bills may create an unnecessary duplicative regulatory burden for credit unions, and we would like to work with you between Committee consideration and Senate consideration to address these concerns.

As you know, credit unions are already subject to very robust data security and data breach notification requirements under the Gramm-Leach-Bliley Act (GLBA), subject to the supervision and enforcement of the National Credit Union Administration (NCUA) or the state supervisory agencies.<sup>1</sup> We appreciate that S. 1151 exempts credit unions which are compliant with GLBA data security requirements from the data security requirements under the bill. With respect to this exemption, we are concerned that the language is somewhat ambiguous as to whether the language exempts state-chartered credit unions. We encourage the Committee to consider a technical amendment to ensure that this language clearly exempts state-chartered credit unions, consistent with what we believe is the intent of the legislation.

We are concerned that neither S. 1151 nor S. 1408 extends a similar exemption to the bills' data breach notification requirements. These requirements, if applied to credit unions, would be largely duplicative of current regulatory requirements and increase the cost of compliance to the detriment of credit unions and their members.

We are also concerned that S. 1151 does not fully preempt states from enacting additional data security and data breach notification requirements. This is an area of law that we feel requires a clear national standard. Many credit unions operate in more than one state; most credit unions have at least some members living in states other than the one in which the credit union primarily operates. Multiple state data security and data breach notifications stands to present credit unions with new, expensive, and possibly inconsistent or conflicting regulatory burden. We are also concerned with the authority that the legislation would give to state attorneys general to enforce the legislation because credit unions are already subject to examination and enforcement of these requirements by the NCUA and state supervisory agencies.

As member-owned financial cooperatives, credit unions place a very significant importance on protecting their members' personal financial information. Credit unions often absorb not only the actual costs, but also the reputational costs, associated with data breaches caused by merchants and other entities, notifying the member that a breach has occurred, canceling and reissuing debit and credit

<sup>1</sup> For state-chartered privately insured credit unions, the Federal Trade Commission is responsible for enforcing compliance with these requirements.



The Honorable Patrick Leahy  
The Honorable Charles Grassley  
September 14, 2011  
Page Two

cards exposed during the breach, and monitoring accounts for fraudulent activity that may have occurred as a result of the breach. Each year, poor security standards or outright negligence on the part of merchants to practice agreed upon security protocols involving electronic payments systems from which they benefit, costs credit unions and their members millions of dollars. We encourage you to consider adding language to this legislation that would make the entity that is subject to a data breach liable for the fraud costs and other costs associated with the data breach. There may be no better enforcement mechanism to ensure merchant compliance with data security standards than to make it clear that they will pay the costs of those affected by their negligence, including credit unions and their members.

We urge the Committee to give these concerns full and fair consideration before moving forward with these or other similar bills, and we look forward to working with you and your staff on these issues.

On behalf of America's 93 million credit union members, thank you very much for your consideration.

Best regards,

A handwritten signature in black ink, appearing to read "Bill Cheney", with a long horizontal flourish extending to the right.

Bill Cheney  
President & CEO