

February 3, 2014

The Honorable Mark Warner
Chairman
Subcommittee on National Security and
International Trade and Finance
Committee on Banking, Housing and Urban
Affairs
United State Senate
Washington, DC 20510

The Honorable Mark Kirk
Ranking Member
Subcommittee on National Security and
International Trade and Finance
Committee on Banking, Housing and Urban
Affairs
United State Senate
Washington, DC 2051

Dear Chairman Warner and Ranking Member Kirk:

On behalf of the Credit Union National Association (CUNA) and America's credit unions, I am writing today to thank you for holding today's hearing entitled "Safeguarding Consumers' Financial Data." CUNA is the largest credit union advocacy organization in the United States, representing America's 6,700 state and federally chartered credit unions and their 99 million members.

This hearing is an important and timely response to recent merchant data breaches affecting millions of Americans and their financial institutions. We appreciate the Subcommittee's focus on safeguarding consumer data, and we look forward to today's testimony and discussion of what should be done to ensure an appropriate response to not only these data breaches, but data breaches that may occur next week, next month, or next year.

We encourage Congress to take a holistic approach to this issue. In the years to come, consumers will use many payment methods, including magnetic (mag) stripe cards, chip and PIN cards (EMV), cloud-based mobile payments, tokenization, and other methods we can only imagine at this point in time. Focusing on one payment method as the absolute answer to solving data security breaches is both shortsighted and distracts from the greater need of a federal data security framework for all entities. Instead, Congress should take a broad look at how consumer data is secured and the improvements that are necessary to prevent future breaches from taking place.

Data breaches occur, in part, because merchants are not required to adhere to the same statutory data security standards that credit unions and other financial institutions must follow, and merchants are rarely held accountable for the costs others incur as a result of the breaches. All participants in the payment process have a shared responsibility to protect consumer data, but the law and the incentive structure today allows merchants to abdicate that responsibility, making consumers vulnerable.

The Honorable Mark Warner
The Honorable Mark Kirk
February 3, 2014
Page Two

Since the initial reporting of the Target data breach, credit unions have focused on protecting their members from harm, to the extent they can. They have taken many steps including, but not limited to, notifying their members that a breach had occurred, reissuing new debit and credit cards to affected members, and increasing staff at call centers to account for additional member inquiries.

The impact of merchant data breach related costs is far reaching; for not-for-profit credit unions operating on already thin margins, these costs make a significant difference in their ability to offer services to their members. CUNA recently conducted a survey of credit unions regarding the costs they are incurring to help their members respond and recover from the recent breach at Target. Preliminary data indicates that credit unions are incurring a cost of approximately \$5.10 per affected card and that the system has incurred a total estimated cost of between \$25-30 million as a result of this breach. This figure will continue to increase because this data does not include fraud costs which may develop in the near future.

In addition to the actual costs credit unions must bear as result of the breach, they also face reputational damage because they have an obligation to notify their members that their account has been compromised but are often limited in their ability to disclose the name of the merchant where the breach occurred. So, when members are notified that their account has been compromised, the credit union is unable to tell them where the compromise occurred and some members assume the problem was with the credit union.

As Congress considers legislative remedies, credit unions support three basic principles:

1. All participants in the payments system should be responsible and be held to comparable levels of data security requirements.

Under current federal law, credit unions and other financial institutions are held to high standards of data security for consumer information under the *Gramm-Leach-Bliley Act*. There is no comparable federal data security responsibility for a national merchant holding consumer data. This represents a weak link in the chain and it needs to be addressed. We support legislation, such as S. 1927, the *Data Security Act of 2014*, introduced by Senators Carper and Blunt, that would provide a national standard for businesses to protect sensitive consumer information, rather than a myriad of differing state laws and regulations.

2. Those responsible for the data breach should be responsible for the costs of helping consumers.

It has been said by merchants that consumers will not be responsible for any financial loss in their accounts. That is true, but not because the merchant will reimburse affected consumers. It happens because the consumer's financial institution pays for the costs related to a merchant data breach involving accounts held at that institution. Under current law, the merchant is not obligated to reimburse financial institutions for any costs incurred as a result of the breach. In other words, even though the breach happened on the merchant's watch,

The Honorable Mark Warner
The Honorable Mark Kirk
February 3, 2014
Page Three

retailers have no responsibility for the costs of the breach because financial institutions take care of their members and customers.

When a merchant data breach occurs, credit unions are there to help their members. Whether it is increased staffing to handle additional member questions, notifying members, reissuing cards, tracking possible fraudulent activity, or reimbursing a member for fraudulent charges caused by a third party, credit unions bear the costs even though the merchant was responsible for the breach. We support legislation to address this problem and make it easier for credit unions to recoup the costs they incur. We believe that if Congress sets strong merchant data security standards and those standards are not met by a merchant whose data is breached, the merchant should be held responsible for the credit union's costs associated with that breach.

3. Consumers should know where their information was breached. Credit unions also support legislation that requires merchants to provide notice to those consumers affected by a data breach, and permits credit unions to disclose where a breach occurs when notifying members that their account has been compromised.

When it comes to bad news like a data breach, it is easy to "blame the messenger." In today's world, the credit union is the messenger and, depending on the state, may not be permitted to identify the breach source to the consumer member. Consumers need transparency and knowledge to understand where their data has been put at risk. S. 1927 addresses this priority as well.

In conclusion, we look forward to the Subcommittee's dialogue regarding data security. It is a complicated and dynamic issue. As these latest merchant breaches have demonstrated, millions of consumers, and their respective credit unions, are affected. We believe the best answer is a federal comprehensive approach to data security.

On behalf of America's credit unions and their 99 million members, thank you for your attention to this very critical matter and your consideration of our views.

Best regards,

A handwritten signature in black ink, appearing to read "Bill Cheney", with a long, sweeping underline that extends to the right.

Bill Cheney
President & CEO