

March 5, 2014

The Honorable Shelley Moore Capito  
Chairman  
Subcommittee on Financial Institutions and  
Consumer Credit  
United States House of Representatives  
Washington, DC 20515

The Honorable Gregory Meeks  
Ranking Member  
Subcommittee on Financial Institutions and  
Consumer Credit  
United States House of Representatives  
Washington, DC 20515

Dear Chairman Capito and Ranking Member Meeks:

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 "Data Security: Examining Efforts to Protect Americans' Financial Information." CUNA is the largest credit union advocacy organization in the United States, representing America's 6,500 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 the recent data breaches, but ones that may occur next week, next month, or next year. We encourage you to hold additional hearings on this matter to address the critical issues facing financial institutions that deal directly with consumers on these breaches.

As we noted in our February 19, 2014, letter to Chairman Hensarling and Ranking Member Waters, a prime reason that merchant data breaches are a chronic issue is because data security standards are inconsistent among the participants in the payments system. Simply put: credit unions and other financial institutions are subject to high data protection standards under the Gramm-Leach-Bliley Act; merchants are not. When merchant data breaches occur, financial institutions – not merchants – bear the costs of replacing credit and debit cards and fraud costs.

The witnesses at today's hearing will focus on how breaches like these happen, how future breaches might be prevented through the deployment of alternative technology and the impact that breaches have on consumers. While we welcome and appreciate this discussion, we are very skeptical that a solution to merchant data breaches can be achieved without addressing the inconsistency in data security standards. Further, until and unless merchants are held accountable for the damages that breaches to their systems cause financial institutions and consumers, we have little confidence that they will be incentivized to

The Honorable Shelley Moore Capito  
The Honorable Gregory Meeks  
March 5, 2014  
Page Two

properly secure their systems. EMV, tokenization and other technologies are critical to the innovation of the payments system; however, the key role for Congress to play in addressing the issue of merchant data breaches is to make sure all of the participants are playing by the same set of rules, and that merchants that permit breaches to occur are responsible for the costs incurred by others.

### **Credit Unions and Other Card Issuers Are Paying the Price for Merchant Data Breaches**

CUNA recently completed our annual Governmental Affairs Conference; merchant data breach was near the top of the list of concerns expressed by our more than 4,400 participants. It is an issue of such great concern because these breaches cost credit unions and their members significantly, and they divert resources from other credit union activity, including lending.

When a data breach occurs, credit unions immediately take steps to protect their members. They know what to do because they have had to do it all too often: they notify their members, make a determination of whether to reissue debit and credit cards, increase call center staff, set up account monitoring, and other activity. These steps are not without cost, however; and 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 bottom line and therefore 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. Based on 1,112 responses to CUNA's Target Breach Survey, representing between a third and 40% of credit union debit and credit cards, credit unions have thus far incurred estimated costs of \$30.6 million. These costs have been predominately for card reissuance and other administrative expense resulting from the breach. Fraud losses, likely to be incurred in the future, will add to the total.

The survey shows that credit unions experienced increased call volumes and increased staffing as a result of the Target data breach. These added to the overall cost to credit unions. CUNA estimates that 4.6 million credit and debit cards were reissued. Credit unions reported two cost items related to the Target breach: card reissuance, and all other costs resulting from the breach (i.e. additional staffing, member notification, account monitoring, etc.). The averages of reported cards per affected card were:

- Card Reissuance: \$3.23 per affected card
- All other costs: \$2.46 per affected card
- Total costs: \$5.68 per affected card

In summary, the data indicate that credit unions incur a cost of approximately \$5.68 per affected card and that the credit union system has incurred a total estimated cost of at least

The Honorable Shelley Moore Capito  
The Honorable Gregory Meeks  
March 5, 2014  
Page Three

\$30.6 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.

Looking to a historical example, in December, 2006, TJX Companies initiated an investigation after discovering suspicious software on its computer systems. The investigation found that for 18 months prior to the investigation, hackers had stolen information dating as far back as 2002 for more than 94 million credit and debit cards.<sup>1</sup> According to the Wall Street Journal, the breach happened as a result of poor wireless network security at the retailer.<sup>2</sup> According to court filings from October 23, 2007: "To date, Visa has calculated the fraud losses experienced by issuers as a result of the breach to be between \$68 million and \$83 million on Visa accounts alone." TJX entered into settlement agreements with Visa and MasterCard. Under the agreement, eligible card issuers received \$40.9 million from Visa and \$24 million from MasterCard. This equates to pennies on the dollar for credit unions who reissued debit and credit cards and did nothing wrong.

### **Congress Needs to Hold Merchants to the Same Standard as Financial Institutions**

Data breaches occur, in part, because merchants are not required to adhere to the same Federal 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.

In addition to the actual costs credit unions must bear as a result of the breach, credit unions 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 may not be able to tell them where the compromise occurred and some members may assume the problem occurred at 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 Federal data security requirements.

---

<sup>1</sup><http://www.pillsburylaw.com/publications/tj-maxx-settlement-requires-creation-of-information-security-program-and-funding-of-state-data-protection-and-prosecution-efforts>

<sup>2</sup> Wall Street Journal: "How Credit-Card Data Went Out Wireless Door."  
<http://online.wsj.com/news/articles/SB117824446226991797>. 4 May 2007.

The Honorable Shelley Moore Capito  
The Honorable Gregory Meeks  
March 5, 2014  
Page Four

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.

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 or assist them with their cards. 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, retailers have no responsibility for the costs of the breach because financial institutions are the ones who 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 state law and other agreements, 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.

The Honorable Shelley Moore Capito  
The Honorable Gregory Meeks  
March 5, 2014  
Page Five

**Conclusion**

Target and Neiman Marcus will not be the last merchant data breaches to capture the headlines unless Congress takes strong steps to enhance data security standards for merchants that accept payment cards. We appreciate that the Subcommittee has an important responsibility to provide leadership in this area, and we will continue to highlight the impact that these breaches have on credit unions and their members as the Subcommittee pursues a remedy to this critical issue.

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 horizontal stroke extending to the right.

Bill Cheney  
President & CEO