

January 27, 2014

Dear Representative:

The recent data breach at Target and other retailers has launched an important conversation about what happens during data breaches, why they happen, who is impacted, who is liable and who should be held responsible. I know that this is an issue many in Congress have taken a great interest in, particularly given its impact on your constituents, and I hope that I can help to shed further light on this complex topic.

As the President and CEO of the Credit Union National Association I feel it necessary to explain the critical role that the financial services industry plays in protecting consumers during breaches as well as to push back on some of the knee-jerk proposals that have been introduced by individuals and organizations who appear to be more interested in playing a blame game than genuinely collaborating on solutions. These breaches are costly for credit unions and – because they are cooperatives –the consumer-members of credit unions who own the institutions. Our primary interest is to protect consumers and work with our partners across industry to develop solutions and prevent future breaches.

Over the past month, tens of millions of Target customers have had their personal information exposed. Credit unions' top priority has been to immediately respond to members regarding any losses, and protect members going forward by taking steps such as reissuing cards and increasing monitoring of accounts.

Credit unions did not wait to determine how the breach occurred or who was at fault. Rather, credit unions took action immediately to ensure the safety and security of their members. These efforts often represent substantial and sometimes crippling costs for credit unions, but these protections are a few of the reasons why consumers, including credit union members, value electronic payments.

Over the past week, I have noticed a disturbing trend of retail trade associations attempting to use this crisis to push policies that they claim would “solve” the problem. I would urge caution when evaluating solutions that appear too good to be true. In reality, cyber security is a complicated issue that has no silver bullets.

First, I would like to address an effort by retail organizations to try and shift both the cost and liability during breaches off of retailers and on to financial institutions, their customers and members, and taxpayers. With regard to liability, some have said that PCI compliance should somehow absolve a retailer of all responsibility. In light of the announcement that massive amounts of other, non-financial consumer data, was accessed at Target, the idea that retailers have no responsibility for protecting consumer data presents a dangerous moral hazard.

Additionally, for the last decade, retailers have done everything in their power to try and slash their financial responsibility for funding the electronic payments system that protects customers and benefits retailers. The so-called Durbin amendment, the most recent example of this campaign, imposed price controls on interchange and thus affected the entire system, necessarily reducing the amount of resources that financial institutions can spend on security. I have to question some retailers' motives when they claim to be concerned about consumers, while actively trying to eliminate a key revenue stream that is used to protect consumers and strengthen the electronic payments system.

With regard to “chip and PIN” technology, which some refer to as a panacea, I have yet to hear a credible explanation of how this technology would have prevented much of this type of breach – it certainly would have no impact on the theft of vast quantities of consumer marketing data, and as long as there is

January 27, 2014

Page Two

unencrypted data at various points in the POS chain, and decryption occurs inside the merchant environment the same vulnerabilities exist. That is not to say that we shouldn't investigate new forms of payments cards, or even that we shouldn't learn valuable lessons from other countries' experiences, but the solution to data breaches is not a simple one and certainly not one that can be resolved by simply switching cards and chasing fraud from face to face transactions into online or "card not present" transactions.

The electronic payments system in the United States safely and securely handles millions of transactions worth billions of dollars every day, while protecting consumers in the rare instance of a data breach, but for it to continue working, we all – credit unions, banks, processors, networks and yes, even merchants – need to do our part.

Data breaches and cyber security are complicated and dynamic issues that will continue to require massive investment and coordination to ensure that consumers are protected. We, as American businesses, can and must do a better job of protecting consumers and their data, but I believe that consumers will be better served by collaborative efforts to solve the tough problems, than by policy decisions that are pitched as a "silver bullet" when in reality, it is far from that simple.

We look forward to working with your office and others as you investigate this complicated topic and steps that can be taken to better protect Americans and their personal information.

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