Credit Union National Association
CUNA

WASHINGTON, D.C.

601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601

Phone: 202-638-5777
Fax: 202-638-7734

TESTIMONY

OF

KIM M. SPONEM
PRESIDENT & CEO
SUMMIT CREDIT UNION

BEFORE THE

FINANCIAL SERVICES SUBCOMMITEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"EXAMINING THE CURRENT DATA SECURITY AND
BREACH NOTIFICATION REGULATORY REGIME"

FEBRUARY 14, 2018

Testimony
of
Kim M. Sponem
President & CEO
Summit Credit Union
Before The
Financial Services Subcommittee on Financial Institutions and Consumer Credit
United States House of Representatives
At a Hearing Entitled,
"Examining the Current Data Security and Breach Notification Regulatory Regime"
February 14, 2018

Chairman Luetkemeyer, Ranking Member Clay, Members of the Subcommittee:

Thank you for the opportunity to testify on this extremely important topic. My name is Kim Sponem and I am CEO and President of Summit Credit Union, headquartered in Madison, Wisconsin. I serve as an ex-officio member of the Credit Union National Association (CUNA) Advocacy Committee on whose behalf I am testifying today.

Summit Credit Union is a state chartered credit union founded in 1935. We serve over 171,000 members and have over $2.9 billion in assets. We would be considered a large credit union. Credit unions range in size from nearly $80 billion in assets to less than $1 million in assets with most being small. In fact, of the nearly 6,000 credit unions in the United States half have less than $30 million in assets and fewer than eight employees, while twenty-five percent have less than $9 million in assets and fewer than three employees. More than 110 million Americans trust credit unions to provide them critical financial services with small credit unions often being the only option for financial services for many Americans. Summit Credit Union offers a full array of financial services to meet the needs of our members. As part of these services, Summit Credit Union offers debit and credit cards to allow our members to purchase goods and services almost anywhere.

Breach Impact on Summit Credit Union and Its Members

Unfortunately, merchant data breaches occur far too often and the cost to Summit Credit Union to cancel and reissue debit and credit cards continues to rise. For example, each year, we receive lists of debit and credit cards that were reported as compromised because of some type of

data breach. These lists could range from one card to many thousands of cards. Summit Credit Union follows specific procedures when notified of a data breach. Staff reviews the listed card numbers as the first step in determining the risk. Staff then decides if the credit union will block and reissue cards or tag the compromised card for additional fraud monitoring. In some cases, the card numbers we receive have already been reported to us (by the member) with fraud on them.

We have been harmed by data breaches occurring at large national merchants such as Target, Home Depot and Equifax as well as at small, local Wisconsin merchants that fail to take necessary steps to protect customer data. For example, in 2016 there was a local card processor that suffered a data breach. This processor routed transactions for a number of restaurants in the Madison area and surrounding communities. During a 4-month period we saw a large spike in fraudulent transactions with our members' credit and debit cards and identified that the common points of purchase were the restaurants that were using the breached processor. However, because we were not notified by this processor that it had been breached, we were required to reissue new credit and debit cards to these members as many as four separate times.

In 2017 alone, we reissued thousands of cards and incurred hundreds of thousands of dollars in losses from card fraud resulting from data breaches. These losses do not include the cost to reissue debit and credit cards or the number of staff hours spent on dealing with our customers' issues with respect to these data breaches. Some of the specific costs my credit union incurs when a data breach occurs at a merchant or processor include:

- Replacing debit and credit cards, which now include EMV or smart chips, the cost of which averages between $3.00 and $5.00 per card;
- Fraud monitoring, which is expensive and labor intensive;
- Addressing member calls and inquires;
- Processing and refunding fraudulent charges; and
- Processing compromised card reissuances.

Additionally, all members whose cards are breached are extremely inconvenienced when they:

- Have to report the fraud and have a new card reissued;
- Have their cards blocked by fraud monitoring so that the member's card is denied when attempting to make a purchase;

- Suffer added stress of knowing fraudsters possess their personal information;
- No longer have access to the use of their credit card when traveling due to it being blocked for fraud;
- Have their debit transactions declined for valid purchases if the fraudster has drained their account; and
- Have to update their automated payments every time their credit card is reissued. We have had several instances where a member forgot to update an automated payment with their new card information and suffered various consequences as the result of late payment.

Recently, we have seen a spike in identity theft. There have been several attempts at loan fraud where fraudsters are using other identities to attempt to obtain loans and open new accounts, which has also increased our costs.

We encourage our members to protect their data by putting a freeze or lock on their credit at the three credit bureaus; however, this takes action on behalf of the member every time they apply for credit and in some cases members incur a cost of $20 to $30 to unlock and relock access to their credit data. This also slows down the loan process and increases costs.

If a member is a victim of identity theft, it takes up a tremendous amount of staff resources to help the member navigate through the process of recovering their identity and rehabilitating their credit history.

We have invested in enhanced procedures in our remote contact areas to identify potential fraudulent activity, both when we review loan and new member applications, as well as with members calling in to conduct business on their accounts. We have also taken active steps to increase education and awareness for our members regarding the potential for card fraud or identity theft. These steps have increased costs to Summit Credit Union in the form of additional staff time to address fraud and support our customers.

Financial institutions, like Summit Credit Union, foot the bill for the fallout and subsequent fraud that comes from the breach of personal information from merchants and other companies' failure to adequately protect and secure customer information. The current state of the law does not put enough responsibility on those handing this sensitive customer information

to properly safeguarding it. Any future legislation must address this lack of responsibility and accountability.

Current Data Breach Landscape

Summit Credit Union is no different than any other financial institution when it comes to the impact it suffers when a data breach occurs. According to the Identity Theft Resource Center, the number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, which is an increase of 44.7 percent over 2016's record high. An annual fraud and risk survey from Kroll's found that in 2017, data theft has surpassed the theft of physical assets.

Without enhanced data security protections for all entities involved in the payments process we are likely to see no slowdown in data breaches in the following years.

Existing Data Security Requirements for Financial Institutions

Title V of the Gramm-Leach-Bliley Act (GLBA) subjects credit unions and banks to data security requirements. GLBA requires financial institutions to develop and maintain procedures and systems to protect consumer information from theft. Breach notification is also part of the GLBA requirements, which require credit unions and banks to notify members and consumers in the event of a breach. Merchants are not subject to similar requirements at the Federal level and the existing state laws do not do enough to protect consumers

Financial institution regulators have promulgated regulations to implement the GLBA requirements. The regulators also supervise financial institutions' compliance with GLBA requirements along with reviewing overall information technology programs for proper data security practices. Credit unions must comply with GLBA and be examined for compliance by a regulator- even the smallest credit unions with one employee.

Credit unions' experience with data security regulations clearly demonstrates that the smallest of businesses can comply with data security and notification requirements and that federal data security requirements would not be too burdensome for small merchants and other businesses. If credit unions and banks of all sizes are required to maintain strong procedures and systems, then merchants and other entities who access and obtain this data should likewise be held to similar standards regardless of size and sophistication.

Strong National Data Security Standard

Americans deserve a strong national data security standard that requires all businesses to protect and safeguard sensitive personal information. Credit unions and their customers will continue to unfairly and unnecessarily incur losses resulting from future data breaches if data security standards are not improved.

As I mentioned above, GLBA provides for requirements that protect members of the smallest to the largest credit unions while allowing these credit unions to operate efficiently. I know that there is concern that small businesses might have difficulty complying with a national data security standard, however small credit unions' ability to comply with the GLBA requirements demonstrates that the smallest businesses can successfully meet data security standards that are properly scaled to their size and risk level. It is important to remember that small businesses purchase credit card processing capabilities from vendors and that these vendors store most of the sensitive data for small businesses. It would seem that these businesses and vendors should be able to bear the responsibility for data security compliance like credit unions do already.

A national data security standard would simplify compliance and notification requirements for businesses. The majority of states and territories have enacted laws governing data security or breach notification. While this patchwork of laws provides some protection for consumers, the differences highlight the need for a baseline national standard. A national standard would ensure that all consumers and financial institutions are protected at least at some level, without preempting any states' right to impose additional requirements.

Strong Notification Requirements

Consumers have the right to know when their personal information has been stolen or lost from a breach or by other means. There is no current federal law that requires merchants or the many others that possess or handle such information to notify consumers or financial institutions when a breach has occurred or within any standard timeframe. Because of the lack of a uniform notification requirement, consumers are often unaware a data breach has occurred and may never learn that their personal information has been stolen or lost. Often, consumers first learn that their personal information has been compromised when their financial institution replaces their debit or credit card. Indeed, many times credit unions like my credit union do not learn of a data

breach until a card processor or card brand notifies us that a breach may have occurred or is covered in the media. This can sometimes be too late to protect the credit union and its members from fraud.

Expedient notification of all stakeholders is a simple and cost-effective way to add a layer of protection to those whose data has been lost and other important stakeholders in the payments ecosystem. It allows consumers and other stakeholders the ability to mitigate possible losses or to address other issues related to a breach. Furthermore, notification also gives consumers the information necessary to protect themselves and enables them to decide whether to keep doing business with a breached entity.

Prompt and uniform consumer notification also assists financial institutions with respect to payment card replacement. Although there are no specific requirements that prevent a credit union from notifying members that a breach has occurred, most may be hesitant to do this because information often is incomplete after a breach. Merchants and other entities that possess payment card and other personal information should take responsibility for their systems and ensure that consumers and other stakeholders are properly notified when a data breach occurs, just as financial institutions are required to do.

Shared Responsibility Costs

CUNA and a number of credit unions, including my credit union, have filed lawsuits to protect other credit unions and their members from harm resulting from the Equifax data breach. The Equifax data breach has harmed and will continue to harm Summit Credit Union, other credit unions, and their members. Hackers had access to highly sensitive personal information and payment card data for months, exposing credit unions to damages in replacing members' payment cards, covering fraudulent purchases, and taking protective measures to reduce the increased risk of identity theft and loan fraud. Credit unions are required to assume financial responsibility for various types of fraudulent activity related to stolen identities and misuse of personal information and payment card data. As the Wall Street Journal just reported on Friday, Equifax submitted a report to the Senate Banking Committee indicating that hackers breached even more information than previously reported, including additional driver's licenses, Tax ID numbers, and email addresses. The lack of any effective data security standards allowed Equifax to ignore the numerous entities who issued public warnings in March 2017 regarding the Apache

Struts vulnerability. Equifax did not update this software to its latest version. In a statement posted September 14, 2017, the Apache Software Foundation attributed the Equifax data breach to Equifax's failure to update this software. Equifax should be held accountable. Any institution that either fails or consciously decides not to implement adequate data security measures should be held accountable to those that they have harmed.

Summit Credit Union is suing Equifax to recover costs and losses directly resulting from the data breach for itself and other credit unions and financial institutions throughout the United States. We also seek to have Equifax take the necessary steps to enhance its current data security to prevent a future breach from occurring. We believe that any business or other entity that possesses or handles consumers' data should be responsible for damage to others resulting from a breach or other loss of this data. My credit union carefully considered litigation as a means to recover from Equifax. Litigation is currently the best way to recover losses stemming from a data breach, and a national standard to hold those entities accountable is warranted.

My credit union and other credit unions need data breach legislation that makes the breached entity responsible to others in the payments ecosystem for losses and other damages that are the result of a data breach. The current system where consumers are protected from loss because financial institutions bear the responsibility for reimbursing their members and customers for losses stemming from data breaches is not fair or sustainable, as the pace and losses from breaches accelerate year after year. Thus, under the current system, financial institutions essentially provide insurance for the entire payments ecosystem while those merchants and other entities whose deficient systems cause the breach, have little incentive to properly safeguard consumers' data because they have no financial incentive or legal requirement to do so.

All participants in the payments ecosystem should be subject to data security requirements and all participants should bear the costs to others from a breach of their system. Properly allocating costs and requirements will cause companies to take action to improve their systems. Enhanced data security requirements will ensure that there is shared responsibility for securing information and costs.

We recognize that data security should be one of the priorities for 2018 and that enhancing payment security to reduce the impact that merchant data breaches have on credit unions and their members is a goal of any proposed legislation. We support strong data security

and data breach notification requirements and will work with policymakers to strengthen the cyber infrastructure to protect consumer data from attack and hold accountable those that fail to adequately protect this information.

On behalf of America's credit unions and their 110 million members, thank you for the opportunity to testify today. I am happy to answer any questions the Subcommittee may have.

Additional Examples of How Breaches Impact Summit Credit Union Members

In addition to the financial harm borne by credit unions and its customers resulting from a data breach, our customers also face significant issues arising from these data breaches. For example, I worked with one member who sent her daughter abroad to study. Her daughter's card was affected by a breach and had fraudulent charges coming through so it was closed. Her daughter was stranded in another country without access to her money. The mother was quite distraught, as you can imagine. She had an email from her daughter but was unable to reach her by phone or text. Imagine having your child stranded with no access to money in a foreign country and almost no way to communicate with her.

We spent a great deal of time coordinating efforts, and we were finally able to send funds via Western Union, communicating with mom and daughter via e-mail.

We had one member who was an over the road truck driver. He was down south and went to fill up his truck and was denied at the pump. He called in a panic as he had a timeline to meet. We did some research for him and found a credit union shared service center a few miles away. He had to drive his semi there, find a place to leave it so he could go in and make a withdrawal. His card had been compromised in a breach, and when fraud occurred his card was shut down.

Another member called in because her daughter's card was involved in a breach and her payment card was shut down for fraud. The mother was furious as the daughter was away at college and had no money to buy food. Her debit card was all she had. As a result of this situation, we rush ordered a card at our expense ($50) to get her daughter a new card the next day. None of these costs are borne by the entities that caused these breaches.

We have had several members who have had their cards blocked while overseas traveling. Sometimes people do not take more than one way to access money when traveling. On more than one occasion we have received emails from members who are panicked as to what to do. We have actually overnighted (again, at our expense) new cards to hotels in other countries. And on at least one occasion, we wired funds to the hotel to pay the hotel bill for a member who could not check out.

Finally, there was a member who was auto-paying her rent with her credit card. When her card was shut down, she forgot to notify her landlord of her new credit card number. When her rent payment was charged to her now-canceled credit card account and rejected, the landlord

notified her that they would only accept a money order going forward. We talked to the landlord and then sent a letter explaining that this was not her fault, she had been a victim of a credit card breach. We were able to get her back in good graces with her landlord.

When a breach occurs, many members want to cancel cards and have new ones reissued because they are so afraid of having fraud occur on their card. They do not understand how this type of fraud can happen, as they have chip cards. They expect their financial institution to protect them from fraud and are angry that their information has been compromised. However, they do not understand that their financial institution had nothing to do with their information being compromised.