



3138 10th Street North  
Arlington, VA 22201-2149  
703.522.4770 | 800.336.4644  
F: 703.524.1082  
nafcu@nafcu.org

National Association of Federal Credit Unions | [www.nafcu.org](http://www.nafcu.org)

March 11, 2015

The Honorable Mitch McConnell  
Majority Leader  
United States Senate  
Washington, D.C. 20510

The Honorable Harry Reid  
Minority Leader  
United States Senate  
Washington, D.C. 20510

The Honorable John Boehner  
Speaker  
U.S. House of Representatives  
Washington, D.C. 20515

The Honorable Nancy Pelosi  
Minority Leader  
U.S. House of Representatives  
Washington, D.C. 20515

**Re: 2015 Verizon Report – 4 Out of Every 5 Global Retailers Fail PCI Test**

Dear Leader McConnell, Leader Reid, Speaker Boehner and Leader Pelosi:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federal credit unions, I write today to bring your attention to the recently released *Verizon 2015 Payment Card Industry Compliance Report*. Massive data breaches at our nation's largest retailers have put millions of consumers at risk and have cost credit unions across the country millions of dollars in fraud related investigations and losses, card reissuance costs, and additional card monitoring. Credit unions and their 100 million members continue to believe Congressional action mandating a strong federal data safekeeping standard for merchants is the only way to prevent breaches and make a meaningful difference for consumers.

The recently released *Verizon 2015 Payment Card Industry Compliance Report* finds that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. In fact, Verizon found that out of every data breach they studied over the past 10 years, not one single company was in compliance with the PCI standards at the time of the breach. This should cause serious pause among lawmakers as failing to meet these standards, exacerbated by the lack of a strong federal data safekeeping standard, leaves merchants, and therefore consumers, more vulnerable to breaches. In addition, the report finds that the use of EMV cards in other countries has not been a silver bullet solution to preventing fraudulent activity, but merely displaces it. The report shows that once EMV use increases, criminals shift their focus to card not present transactions, such as online shopping. NAFCU has long argued that any breach notification standards must be accompanied by strong data safekeeping standards for merchants akin to what credit unions comply with under the *Gramm-Leach-Bliley Act* (GLBA).

Merchants and credit unions are both targets of cyberattacks. The difference, however, is that credit unions have developed and maintain robust internal protections to combat these attacks and are required by federal law and regulation to protect this information and notify consumers when a breach occurs that will put them at risk. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A

credit union faces potential fines of up to \$1 million per day for compliance violations. These extensive requirements and safeguards have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999 as part of GLBA. In contrast, retailers are not covered by *any* federal laws or regulations that require them to protect the data and notify consumers when it is breached.

The ramifications for credit unions and their members have been monumental. A February 2015 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were \$226,000 on average. Of their losses, respondents expect to recoup less than .5% which amounts to less than \$100 on average. Despite the claims of some trade groups, the fact remains that our members are not recovering anything close to what they are spending to make their members whole after a merchant breach.

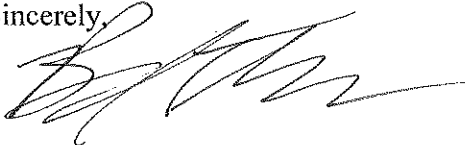
NAFCU urges Congress to come together in a bipartisan way and put forward legislative recommendations to hold retailers to the same strict standards of cybersecurity and data security that financial institutions must already adhere to. NAFCU recommends that legislation address:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.
- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *Gramm-Leach-Bliley Act*.
- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

On behalf of our nation's credit unions and their 100 million members we thank you for your attention to this important matter. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Director of Legislative Affairs, Jillian Pevo, at (703) 842-2286.

Sincerely,



Brad Thaler  
Vice President of Legislative Affairs

cc: Members of the United States Senate  
Members of the United States House of Representatives