Testimony of

Jan N. Roche

President and CEO

State Department Federal Credit Union

on behalf of

The National Association of Federal Credit Unions

The EMV Deadline and What it Means for Small Businesses

Before the

House Small Business Committee

October 7, 2015

Introduction

Good morning, Chairman Chabot, Ranking Member Velázquez and Members of the Committee. My name is Jan Roche and I am testifying today on behalf of the National Association of Federal Credit Unions (NAFCU). I serve as the President and CEO of State Department Federal Credit Union (SDFCU), headquartered in Alexandria, Virginia, and also serve on the Board of Directors of NAFCU. I have over 30 years of experience in credit union and financial management.

State Department Federal Credit Union was chartered in 1935 through the efforts of eight employees of the Department of State. Now, 80 years later, we serve over 67,000 members worldwide and have over $1.6 billion in assets. Due to the traveling habits and job assignments of many of our members and the fact that 8 percent of our membership is located overseas at any given time, we were one of the first financial institutions in the U.S. to start issuing EMV VISA Credit Cards in June, 2012.

As you are aware, NAFCU is the only national organization exclusively representing the federal interests of the nation's federally-insured credit unions. NAFCU-member credit unions collectively account for approximately 70 percent of the assets of all federal credit unions. We appreciate the opportunity to appear before you today to talk about the EMV transition deadline in the United States and the need for data security legislation, including H.R. 2205, the *Data Security Act of 2015*.

Background on Credit Unions

Historically, credit unions have served a unique function in the delivery of essential financial services to American consumers. Established by an Act of Congress in 1934, the federal credit union system was created, and has been recognized, as a way to promote thrift and to make financial services available to all Americans, many of whom may otherwise have limited access to financial services. Congress established credit unions as an alternative to banks and to meet a precise public need – a niche that credit unions still fill today.

Every credit union, regardless of size, is a cooperative institution organized "for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes." (12 USC 1752(1)). While over 80 years have passed since the Federal Credit Union Act (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- credit unions remain wholly committed to providing their members with efficient, low-cost, personal financial services; and,
- credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

Credit unions are small businesses themselves, especially when compared to our nation's mega banks and largest retailers, facing challenges of meeting the products and service needs of their community, while dealing with various laws and regulations.

EMV

EMV is the established global standard for "chip" cards and their compatibility with point of sale terminals. EMV stands for "EuroPay, Mastercard and VISA," the three companies that created the standard. EMV cards are still plastic, but they contain an embedded microprocessor (or "chip") that stores data and adds additional protection by making it harder to produce a counterfeit card that can be used at a point of sale terminal. This is because the chip generates unique data (a new, random number) for each transaction. If that data is stolen, it is not traceable back to the account. It is important to understand that it is this EMV "chip" technology that makes the new cards more secure – not a PIN or signature. It is also important to recognize that the EMV solution is the new market standard for combating fraud at the point-of-sale and assigning liability when a fraudulent credit card is used. It is not a "silver bullet" solution to the broader problem of data security or to combat online identity theft.

EMV is just one step in a larger universe of measures that credit unions take to protect the financial data of their members (consumers) and the payments system. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA) and are innovators in the ever-developing payments system as they strive to protect the financial information of the 101 million Americans who are credit union members.

My testimony today will cover how credit unions are protecting consumers in the payment system, the impact of the EMV transition and what steps are needed to better protect consumer financial data moving forward.

NAFCU's Work in Various Cyber and Data Security Initiatives

NAFCU is pleased to be an active participant in various industry and government payments, cyber and data security initiatives, doubling down these efforts as data breaches continue to rise and innovations in payments technology make the entire ecosystem more complex for financial institutions and consumers.

Specific to payments, NAFCU is a member of the *Payments Security Task Force*, a diverse group of participants in the payments industry that is driving a discussion relative to systems security. NAFCU also supports many of the ongoing efforts at the *Financial Services Sector Coordinating Council* (FSSCC) and the *Financial Services Information Sharing and Analysis Center* (FS-ISAC). These organizations work closely with partners throughout the government creating unique information sharing relationships that allow threat information to be distributed in a timely manner.

NAFCU also worked with the *National Institute of Standards and Technology* (NIST) on the voluntary cybersecurity framework released in 2013 designed to help guide financial institutions of varying size and complexity through the process of reducing cyber risks to critical infrastructure. The recommendations are designed to evolve and will be updated to keep pace with changes in technology and threats.

Earlier this year, NAFCU also participated in President Barack Obama's *White House Summit on Cybersecurity and Consumer Protection* at Stanford University which featured leaders from across the country—industry, tech companies, law enforcement, consumer and privacy

advocates, law professors who specialize in this field, and students — to collaborate and explore partnerships that will help develop the best ways to bolster cybersecurity. Credit unions continue to pursue greater data security through innovation.

During the Summit, NAFCU-member First Tech Federal Credit Union's recent partnership with MasterCard in the area of card security was announced. First Tech is innovative in this area and is implementing a new pilot program this year that will allow consumers to authenticate and verify their transactions using a combination of unique biometrics such as facial and voice recognition. This type of innovation is a generation beyond EMV, and is not unusual at member-owned and member-driven credit unions as we take data security seriously. Technological innovations like this are a prime example of why Congress needs to ignore calls to legislate technological solutions, which can soon become out-of-date, rather than creating basic standards of data protection.

NAFCU is also a participant in the Federal Reserve's initiative to improve the U.S. payments systems through two industry taskforces launched earlier this year: the Faster Payments Taskforce and the Secure Payments Taskforce. Through the Faster Payments Taskforce, NAFCU is working with the Federal Reserve and industry participants to create criteria to identify and evaluate alternative approaches for implementing safe, ubiquitous, faster payment capabilities. Additionally, on the Secure Payments Task Force, NAFCU is providing input to the Federal Reserve on payment security matters and is helping determine priorities for future action to advance payment system safety, security and resiliency.

The EMV Transition

October 1, 2015, was the deadline established by the four major U.S. credit card issuers (Mastercard, Visa, Discover and American Express) when the liability for the majority of card-present fraudulent transactions on credit cards is shifted to whichever party is not EMV-compliant. Given the nature of our field of membership, which includes many State Department employees that travel or are stationed overseas in countries where the EMV transition has already occurred, SDFCU was an early adapter to the U.S. transition, first issuing EMV cards in June of 2012 for new cards and replacements for lost and stolen cards. Our credit card portfolio of over 28,000 cards is now 100% EMV.

It is important to note that the EMV transition in the U.S. is a voluntary one established by the market, and not a government mandate. The October 1, 2015, deadline is not the endpoint of transition, rather just a step along the road of progress when the incentives to be EMV-compliant changed. Companies have not been forced to transition (whether it's issuing or accepting EMV cards) if they are willing to bear the liability. The speed of shifting to EMV is essentially a business decision that is dependent on risk-tolerance. It is important to note that, whether or not a card or business is EMV-compliant, consumers are not liable for fraud losses as all credit cards have zero liability provisions for consumers and the *Electronic Funds Transfer Act* limits consumer liability for any fraud on debit cards. Consumers remain protected in the new system.

Based on a NAFCU survey of our members, a majority of credit unions are ready for the EMV transition and are issuing EMV credit cards to their members as they issue new cards or replace older magnetic-stripe cards. There is a greater cost for an EMV card for credit unions. At

SDFCU, the cost (not including staff costs, set up and postage) to produce a non-EMV card is approximately $3.04 and to produce a new EMV card it is approximately $5.81.

A comprehensive study released September 17, 2015, by the Strawhecker Group reported that only 27% of merchants were to be EMV-ready by October 1, 2015. In other recent surveys, the reasons given by merchants for not being ready include: not knowing about the transition (despite it being several years in the works), not wanting to pay for an EMV terminal, not being concerned about the liability shift and thinking that the EMV shift is unfair. Many of these are small and mid-size businesses that could find themselves the next targets of data thieves that will seek to exploit this vulnerability in the payment system as many big box retailers make the conversion. We believe that successful protection of the payments system requires all parties to be actively involved and hope that these businesses will work with the financial services community to recognize their role in making the payments system safer.

The PIN Debate

Some have argued that the EMV transition should have included a PIN mandate to require consumers to enter PINs for every transaction. Imposing such a mandate or requirement would be unrealistic and would not be a panacea for the problem of data security. As I noted earlier, it is the chip technology that makes new cards secure, not the PIN or signature. A PIN is a static data element that is still vulnerable to theft. If it is compromised, a consumer's entire account can be put at risk. A 2012 report by the Federal Reserve Bank of Atlanta found that PIN fraud rates had increased significantly since 2004. A PIN mandate would not have helped prevent recent major consumer data breaches such as Target, Home Depot and Michaels.

A PIN mandate also does not prevent online or mobile fraud, often referred to as "card-not-present" fraud, which is already 45% of card fraud in the U.S. according to the Aite Group (at SDFCU in the last year, it was about 40% of our gross card fraud). This type of fraud is also expected to rise significantly after the EMV transition. Wider use of PINs in other EMV countries has done nothing to prevent spikes in card-not-present fraud. In the United Kingdom, online fraud rose 79% after their EMV transition. In Canada, while card-present fraud declined after the switch to EMV, card-not-present fraud more than doubled.

A truly secure payments system must be one that is constantly evolving to meet emerging threats and uses a wide range of dynamic authentication technologies – EMV, tokenization, encryption, biometrics and more. Many retailers today are increasingly moving away from traditional point-of-sale authentication methods, like PIN or signature, and relying on network-based monitoring to identify fraud as it can improve the customer experience by reducing time spent in the checkout line. Many of you may have experienced transactions where the merchant does not request a signature nor PIN with card usage. Retailers have demanded this change of the industry to speed the checkout process. Because retailers do not have standards requiring them to protect consumer data collected at the point of sale, they have sometimes prioritized the speed of the transaction to increase customer sales at the expense of the security of the payments system. This can make retailers a vulnerable point of entry to data breaches in the payments ecosystem, even with PIN and signature authentication.

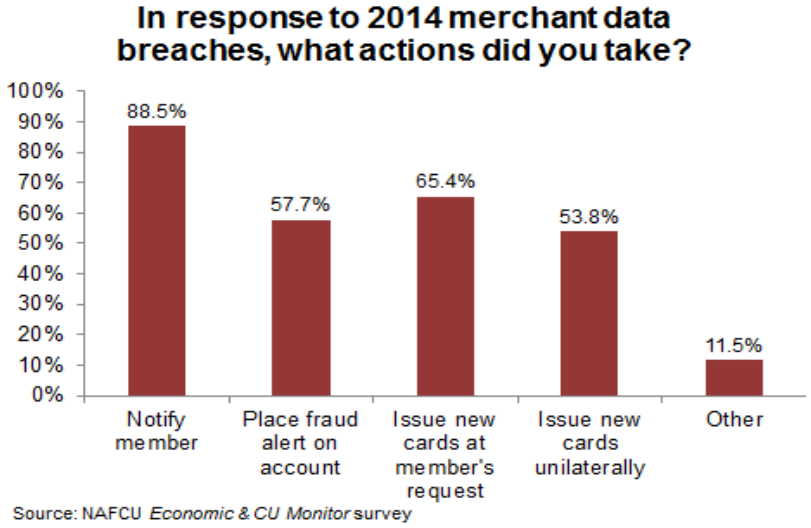
Credit Unions and Consumers Suffer in Data Breaches

The EMV transition is not a silver bullet to addressing the scourge of data breaches. More needs to be done to establish a national standard for protecting the financial data of consumers. Americans are becoming more aware and more concerned about data security and its impact. A Gallup poll from October, 2014, found that 69 percent of U.S. adults said they frequently or occasionally are concerned about having their credit card information stolen by hackers, while 27 percent of Americans say they or another household member had information from a credit card used at a store stolen in the last year. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

Data security breaches are more than just an inconvenience to consumers as they wait for their plastic cards to be reissued. Breaches often result in compromised card information leading to fraud losses, unnecessarily damaged credit ratings, and even identity theft. Symantec's *Internet Security Threat Report* issued earlier this year found that 36% (roughly 74 million consumers) of the over 205 million individuals compromised in retail breaches in 2014 had their financial information exposed. That percentage doubled from 18% in 2013. More than 23% of the US population had their financial identities compromised by a retailer data breach in 2014.

While the headline grabbing breaches are certainly noteworthy, the simple fact is that data security breaches at our nation's retailers are happening almost every day. A survey of NAFCU member credit unions, found that respondents were alerted to potential breaches an average of 164 times in 2014. Two-thirds of the respondents said that they saw an increase in these alerts from 2013. When credit unions are alerted to breaches, they take action to respond to protect

their members. The chart below outlines the actions that credit unions took in 2014 in response to merchant data breaches.



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. 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.

Credit Unions and GLBA

As I noted above, credit unions, and all financial institutions, are subject to the 1999 *Gramm-Leach-Bliley Act*. GLBA and its implementing regulations have successfully limited data breaches among financial institutions and this standard has a proven track record of success since its enactment. This record of success is why we believe any future requirements must recognize and incorporate this existing national standard for financial institutions such as credit unions.

Consistent with Section 501 of the GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLBA and its implementing regulations have successfully limited data breaches among credit unions. NAFCU believes that the best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or

contradictory, data security regulations for financial institutions already in compliance with GLBA.

There are a number of key elements, requirements and definitions of the GLBA that apply to credit unions and are outlined below. The GLBA directed regulators to establish evolving standards for financial institutions to ensure the security and confidentiality of consumer information.

The GLBA also sets a number of important definitions and requirements:

Sensitive Consumer Information
Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log into or access the member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

Unauthorized Access to Consumer Information
The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

Risk Assessment and Controls
The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business. This is a critical aspect of GLBA that allows flexibility and ensures the regulatory framework is workable for the largest and smallest in the financial services arena. As the committee considers cyber and data security measures, it should be noted that scalability is achievable and that it is a misnomer when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying size businesses.

At a minimum, the credit union is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to consumer information;
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies;
- Train staff to implement the credit union's information security program; and,
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."

Service Providers

The security guidelines direct every financial institution to require its service providers through contract to implement appropriate measures designed to protect against unauthorized access to, or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events,

cost savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

An institution that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

Response Program

Every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. **The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.**

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers. Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

Consumer Notice

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good consumer relations, and enable the institution's members to take steps to protect themselves against the consequences of identity theft.

Content of Consumer Notice

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected fraud or identity theft to the institution.

Delivery of Consumer Notice

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

Preventing Future Breaches

While financial institutions are subject to the robust standards of the GLBA outlined above, retailers and others who handle financial data are not subject to the same type of national standard. NAFCU has long argued that protecting consumers and financial institutions by preventing future data breaches hinges on establishment of strong federal data safekeeping standards for retailers and merchants akin to what credit unions already comply with under the GLBA. NAFCU has developed a number of key principles that should be considered and incorporated in the data security debate (Appendix A). Unfortunately, merchants have attempted to use the EMV and PIN debate to stop any meaningful discussion about data security legislation—thus not addressing the real issue of the broader responsibility of merchants to protect consumers' financial data.

The time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Such a standard must recognize the existing protection standards that financial institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach.

While some have said that voluntary industry standards should be the solution, the recently released *Verizon 2015 Payment Card Industry Compliance Report* found 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, <u>not one single company was in compliance with the PCI standards at the time of the breach.</u> 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.

One basic but important concept to point out with regard to almost all cyber and data threats is that a breach may never come to fruition if an entity handling sensitive information limits the amount of data collected on the front end and is diligent in not storing sensitive personal and financial data in their systems. Enforcement of prohibition on data retention cannot be over emphasized and it is a cost effective and commonsense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of cyber criminals.

Legislative Solutions

NAFCU believes that the best legislative solution on the issue of data security that has been introduced in this Congress is the bipartisan legislation introduced by Representatives Randy Neugebauer and John Carney, H.R. 2205, the *Data Security Act of 2015*. This legislation creates a national data security standard that is flexible and scalable, does not mandate static technology solutions and recognizes those who already have a working standard under the GLBA. We support this legislation and would urge you to support it as well.

Conclusion

Cyber and data security, ensuring member safety, and incentivizing data safekeeping in every link of the payments chain is a top challenge facing the credit union industry today. A truly secure payments system must be one that is constantly evolving to meet emerging threats and uses a wide range of dynamic authentication technologies – EMV, tokenization, encryption, biometrics and more. When it comes to EMV, what matters most is the chip technology that

makes the cards more secure. Requiring additional measures such as PIN usage does not make substantial improvements to the system. While credit unions are largely ready for the EMV transition, wider adoption of EMV technology by others in the payment system, such as retailers, will only strengthen the system. Still, more needs to be done.

Consumers will only be protected when every sector of industry is subject to robust federal data safekeeping standards that are enforced by corresponding regulatory agencies. It is with this in mind that NAFCU urges Congress to modernize data security laws to reflect the complexity of the current environment and insist that retailers and merchants adhere to a strong federal standard in this regard. Enacting H.R. 2205, the *Data Security Act of 2015*, would be an important step toward this goal.

Thank you for the opportunity to appear before you today on behalf of NAFCU. I welcome any questions you may have.

Appendix A

NAFCU's Key Data Security Principles

- **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 the GLBA, 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 the GLBA 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 *GLBA.*

- **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.