Testimony of

James E. Mooney

President & CEO

Chevron Federal Credit Union

on behalf of

The National Association of Federally-Insured Credit Unions

“Small Business Cybersecurity: Federal Resources and Coordination"

Before the

House Small Business Committee

March 8, 2017

Introduction

Chairman Chabot, Ranking Member Velázquez and Members of the Committee, thank you for the invitation to appear before you this morning. My name is Jim Mooney and I am testifying today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU). I am the President and CEO of Chevron Federal Credit Union, headquartered in Oakland, California, and also serve as Chair of NAFCU's Cybersecurity and Payments Committee.

Chevron Federal Credit Union is a federally charted credit union serving the employees of Chevron Corporation, Bechtel Corporation, and numerous smaller companies as well as retirees and family members. We serve 107,000 members through 21 branches located in California, Texas, Utah, Louisiana, Mississippi, and Virginia.

As you are aware, NAFCU is the only national organization exclusively representing the interests of the nation's federally-insured credit unions. NAFCU-member credit unions collectively account for approximately 70 percent of the assets of all federally-insured credit unions. It is my privilege to submit the following testimony on behalf of NAFCU, our credit unions and the 100 million members they represent that have been heavily impacted by ongoing data security breaches by no fault of their own. We appreciate the opportunity to speak about how cybersecurity and data security issues impact credit unions.

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.

Credit Unions and Data Security

Today, my testimony will cover credit union efforts to maintain a successful track record of protecting member information, NAFCU's work on the cyber and data security front, the impacts

of recent retailer and merchant data breaches on credit unions and consumers, including the financial burdens they have faced, and NAFCU's principles for data security reform and potential legislative next steps to address consumer data threats that exist in the 21st century cyber environment.

As members of the committee are well aware, cyber and data crime has reached epic proportions in nearly all sectors of the economy. Symantec's *2016 Internet Security Threat Report* characterized 2015 as a year when "attacks against businesses and nations hit the headlines with such regularity that we've become numb to the sheer volume and acceleration of cyber threats." According to the report, more than 430 million new pieces of malware were created in 2015 and the number of identities exposed in breaches increased by 21 percent from 2014. While large companies across all sectors are still a prime target, 65 percent of all targeted attacks struck small and medium-sized companies last year.

In a recent report by Javelin Strategy & Research, they found that card not present fraud increased by 40% from 2015 to 2016. The author of the report, Al Pascual, head of security, risk, and fraud at Javelin Strategy & Research noted that the jump in fraud was not simply the shift of card present to card not present fraud, but pointed to the online retailers and merchants not maintaining up-to-date security standards. My credit union's experience is consistent with the report's findings: in the four-year period of 2013 to 2016 -- during which we implemented EMV -- our card-related fraud losses tripled, with 2016 losses approaching three-quarters of a million dollars.

With cyber and data crime becoming more and more prevalent the U.S. government is also working to identify malicious actions within their networks. In 2015 the Department of Homeland Security's Office of Cybersecurity and Communication announced that a network monitoring program would fully cover the government by the end of fiscal year 2016 through the Einstein program used to strengthen perimeter defenses and the Continuous Diagnostics and Mitigation program designed to better detect hackers once systems have already been penetrated. In 2015, Senators Tom Carper and Ron Johnson introduced S. 1869, the Federal Cybersecurity Enhancement Act, which included language authorizing the Department of Homeland Security to use the Einstein program on every federal agency's network. Language from the bill was included in the Cybersecurity Act of 2015, which was a Division N of the omnibus passed in December of 2015 and does not sunset till 2022. As the cybersecurity conversation moves forward we believe that it is important for Congress to also explore industry improvements that can and need to be made regarding data security standards.

NAFCU supports comprehensive data and cybersecurity measures to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA). Unfortunately, there is no comprehensive regulatory structure similar to what GLBA put in place for financial institutions for other entities that may handle sensitive personal and financial data.

In today's digital economy, cybersecurity poses a threat to businesses of all sizes, individual consumers, and even national security. From the financial services perspective, cybersecurity and data security are inextricably linked. Securing consumers' personal information and financial

accounts will require the entire payments ecosystem to take an active role in addressing emerging threats, and in turn require all industries to be proactive in protecting consumers' personally identifiable and financial information from the onset.

As will be discussed in my testimony, credit unions have been able to successfully minimize emerging threats and data breaches. Still, consumers unintentionally put themselves at risk every time they use their debit or credit card. Given the magnitude of the many recent data breaches and the sheer number of consumers impacted, policy makers have a clear bipartisan opening to ensure all industries in the payments system have a meaningful federal data safekeeping standard to help prevent further breaches from occurring.

This hearing is an important one as we are at a critical juncture in the cyber and data security discussion on Capitol Hill. On behalf of NAFCU and our member credit unions, I appreciate the opportunity to be here today.

Financial Institutions and the *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 protecting valuable information since its enactment in 1999. This record of success is why NAFCU believes any future requirements must recognize 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. The best way to move forward and address data breaches is to create a comprehensive regulatory strategy for industries that are not already subject to oversight with the responsibility of protecting consumer data. 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.

Below, I outline the key elements, requirements and definitions of the GLBA. Specifically, the GLBA:

- Requires financial institutions to establish privacy policies and disclose them annually to their customers, setting forth how the institution shares nonpublic personal financial information with affiliates and third parties.
- Directs regulators to establish regulatory standards that ensure the security and confidentiality of customer information.

- Permits customers to prohibit financial institutions from disclosing personal financial information to non-affiliated third parties.
- Prohibits the transfer of credit card or other account numbers to third-party marketers.
- Prohibits pretext calling, which generally is the use of false pretenses to obtain nonpublic personal information about an institution's customers.
- Protects stronger state privacy laws and those not inconsistent with these federal rules.
- Requires the U.S. Department of Treasury and other federal regulators to study the appropriateness of sharing information with affiliates, including considering both negative and positive aspects of such sharing for consumers.

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 applicable 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 is inaccurate 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 financial institution 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.

Regulators Oversight of Financial Sector Cybersecurity

Since the passage of GBLA, financial regulators have developed robust guidance to help institutions develop information security programs and enterprise risk management policies to address data and cybersecurity needs. In addition, financial regulators oversee bank and credit union cybersecurity through periodic examinations designed to assess the risks associated with IT environments of varying size and complexity.

Guidance promulgated by the Federal Financial Institutions Examination Council (FFIEC) has shaped the contents of bank and credit union examinations. In June 2015, the FFIEC publicly announced its Cybersecurity Assessment Tool (CAT), which was influenced in large part by the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), released by the

National Institute of Standards and Technology ("NIST") in 2014. Both the Framework and the CAT are voluntary tools that credit unions and banks can use to gauge their cybersecurity readiness. The Framework has endowed the CAT with a common lexicon of cybersecurity terminology, which has also influenced the thinking of other financial institution regulators. Furthermore, NCUA has said that its ongoing update of IT examination procedures will adhere to the principles described in the CAT, and other financial regulators have either aligned their cybersecurity standards more closely with the Framework or voiced support for its risk-based approach.

Financial sector cybersecurity has always been a priority for banking and credit union regulators; however, in recent years it has emerged as top issue. NCUA has made cybersecurity a supervisory priority since 2013, and the agency reminded credit unions in 2016 that "technological innovation, the expansion of social networking and growing interconnectivity are fueling fundamental change in cybersecurity procedures and processes." NCUA forecasts that elevated risk levels may lead to "higher mitigation costs and lower consumer confidence, as well as greater financial and legal risks." Likewise, other regulators have either announced changes to their own examination procedures as a result of growing technological complexity in the financial sector, or issued new proposals aimed at mitigating unprecedented levels of data security risk.

Government Resources for Managing Data and Cybersecurity Risk

Credit unions and banks have benefited from the availability of government initiatives aimed at coordinating information sharing, identifying emerging threats, and promoting greater cybersecurity expertise. A NAFCU survey released in October 2016 revealed that members use government resources such as the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center, the U.S. Department of Treasury's Financial Crimes Enforcement Network, NIST's National Vulnerability Database, and the United States Computer Emergency Response Team (US-CERT) to maintain awareness of emerging data security threats and develop stronger cybersecurity standards. To support interagency coordination across these platforms, NAFCU has engaged the Treasury Department Office of Critical Infrastructure Protection and Compliance Policy to suggest areas of improvement and future opportunities for public-private collaboration.

NAFCU's Work in Various Cyber and Data Security Initiatives

In addition to these government platforms, many credit unions and banks belong to industry-led organizations such as the Financial Services-Information Sharing and Analysis Center (FS-ISAC), of which NAFCU is a member. As data breaches continue to rise and innovations in payments technology make the entire ecosystem more complex for financial institutions and consumers, involvement in these organizations is as critical as ever.

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.

Information sharing is a key weapon in credit unions' arsenal against cybercrime. NAFCU has long held that cyber threats could be mitigated with a greater level of collaboration between financial institutions, and the use of public-private partnerships to share information about threats and cybersecurity best practices. To that end, NAFCU has recently collaborated with FS-ISAC to promote awareness of a new information sharing initiative specific to credit unions. FS-ISAC has spoken to NAFCU's Cybersecurity and Payments Committee about its recently launched Credit Union Advisory Council, which allows member credit unions to share critical insights about emerging data security threats, consult model risk assessments, and gain insights on nearly every aspect of cyber risk management. NAFCU believes that interest in FS-ISAC's advisory council, as well as other credit union led information sharing organizations, demonstrates that credit unions are keenly aware of the fast-evolving threat environment that threatens the financial sector.

NAFCU has also aided industry efforts to make data security effective not just for institutions but also for consumers. In November of 2016, FS-ISAC released its "Sheltered Harbor" initiative to improve cybersecurity defense measures for financial institutions. The creation of Sheltered Harbor came as a response from cybersecurity exercises that FS-ISAC members participated in over this past summer. In the case of potential cyber incidents, Sheltered Harbor would allow financial institutions to securely store member account information in data vaults so it can be protected and restored. NAFCU has provided assistance to support the development and maintenance of the Sheltered Harbor program because it understands the critical importance of

cybersecurity. In today's challenging cyber environment it is important that those who have access to significant customer information look for ways to enhance consumer protections.

NAFCU also worked with NIST on the Framework it released in 2014 which has since guided 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.

NAFCU's efforts to gauge credit union cybersecurity readiness indicate that the vast majority of members have taken a proactive approach to managing data security risks and improving operational resilience. A NAFCU survey published October 2016 revealed that 93.7 percent of survey respondents reported that their credit union participates in some form of information sharing to keep pace with cybersecurity threats, and nearly 70 percent of respondents make use of NIST's National Vulnerability Database to track and monitor common vulnerabilities. NAFCU's survey also showed that the percentage of respondents' overall operating budget devoted to IT/cybersecurity has nearly doubled over the past five years. In addition, to address growing cybersecurity risks, a quarter of all respondents have hired a Chief Information Security Officer to manage cybersecurity-related activities. Meanwhile, half of all respondents have a committee specifically devoted to cybersecurity oversight, and an additional 6.3 percent of respondents have added cybersecurity oversight to their board of directors' or supervisory committee's existing duties.

Protecting Consumer Data is Important

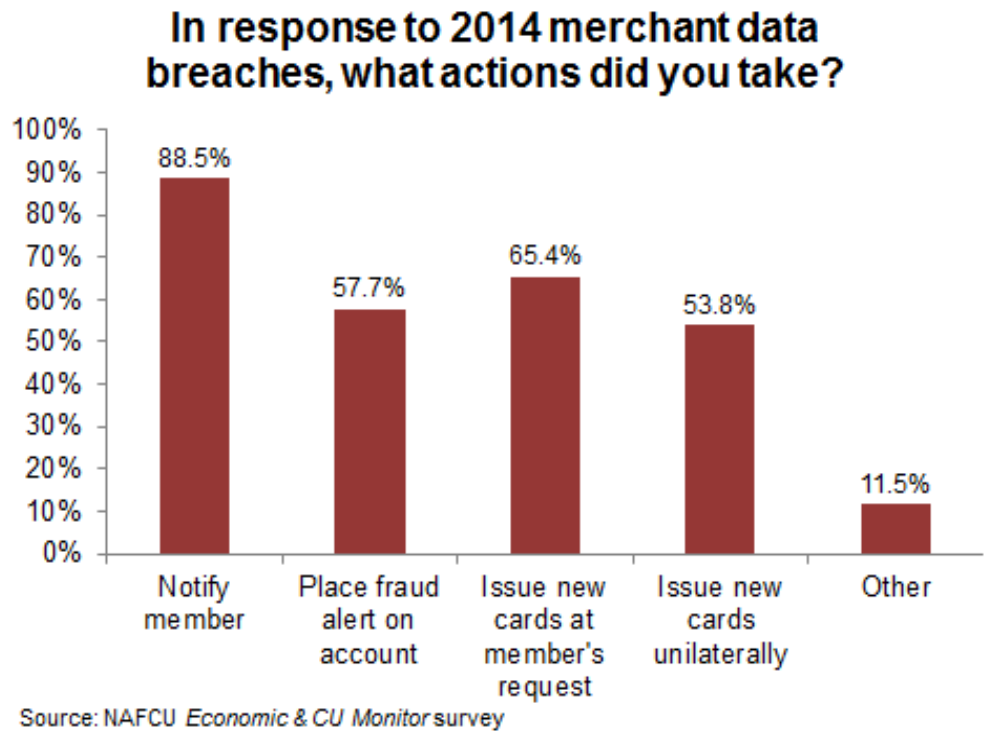
With the increase of massive data security breaches at retailers, from the Target breach at the height of holiday shopping in 2013 impacting over 110 million consumer records to the 2014 Home Depot breach impacting 56 million payment cards, Americans are becoming more aware and more concerned about data security and its impact. A Gallup poll from October 12-October 15, 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 according to an October 2016 Gallup survey. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

Since the large Target and Home Depot breaches there have been many others including the most recent breaches at Wendy's and Arby's fast-food chains. The Arby's breach, which was announced just last month, has so far compromised 355,000 customer credit cards and the investigation is still developing. NAFCU-member, Evansville Teachers Federal Credit Union reported that the Arby's breach impacted 5,214 of their card holders. To shut off the member's breached card, cover the reported fraud, and pay for the card reissue it cost Evansville Teachers Federal Credit Union alone a total of $52,466.10. With the Arby's breach investigation still unfolding and its known impacts on so many financial institutions already, it is unclear how many more credit unions have or will face similar costs.

Data security breaches are more than just an inconvenience to consumers as they wait for their debit and/or credit 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 in April of 2016 found that individuals' financial

information was exposed in 33% (over 140 million) of the 429 million records compromised in the 2015 breaches . That percentage is up significantly from 18% in 2013. More than 23% of the US population had their financial identities compromised by a merchant 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 in February of 2015, 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 respond and protect their members. The chart below outlines the actions that credit unions took to respond to data breaches in 2014.



Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum federal standards for protecting such data.

Retailers and credit unions are both targets of cyberattacks. The difference, however, is that credit unions have developed and maintained robust internal protections to combat these attacks and are required by federal law and regulation to protect this information as well as notify their members when a breach occurs, putting 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 discussed earlier in my testimony have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999. In contrast, retailers are not required by ***any*** federal laws or regulations to protect the consumers' data and notify them when it is breached.

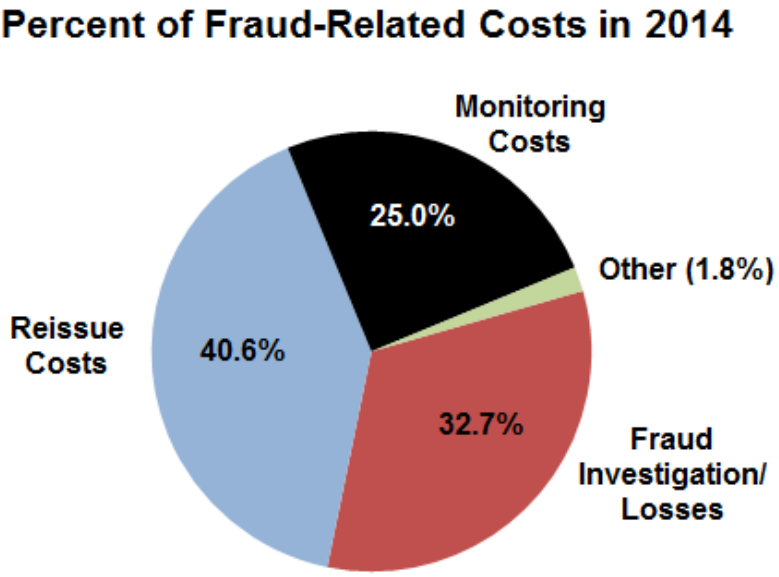
A credit union data security program to protect its own system can have many security components, such as:

1. Firewall
2. Intrusion Prevention

3. Botnet Filtering
4. Anti-Virus protection
5. Malware protection
6. Management and Monitoring Services
7. Anti-Phishing and Phishing site takedown services
8. Third party vulnerability assessments and testing
9. Web Filter
10. Spam Filter
11. Secure Email
12. Encryption
13. End point security

These elements can have a significant cost to the institution. A February, 2015, survey of NAFCU members found that the average respondent credit union spent $136,000 on data security measures in 2014, which does not even factor in the additional costs that the credit union faced due to data breaches at other entities.

The ramifications of recent data breaches for credit unions and their members have been monumental. The aforementioned survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were $226,000 on average per credit union. Almost all respondents noted that merchant data breaches lead to increased member-service costs and needs that are not reflected in these direct costs. The three main elements of these costs were card reissuing costs, fraud investigations/losses and account monitoring. The chart on the next page outlines how these various costs from merchant data breaches are broken down.



The data breaches in 2014 for the credit union I serve as President and CEO, Chevron Federal Credit Union, were estimated to have cost us $294,804. From 2013 through 2016 data breaches have cost my credit union an estimated total of $833,000 in member notification and card resissue expenses. This does not even include the actual fraud losses. These costs are almost double what Chevron Federal Credit Union pays to annually for information security systems and services, which does not include the costs of our three-person IT Information Security team.

Another cost, though difficult to measure: members often do not know that their compromised cards are due to a specific data breach. The card networks do not identify the compromise sources in their card alerts. Therefore, credit union staffs typically can only inform affected members that their cards may be compromised, not the source of the compromise. For all the members know, the source of the problem may be the credit union itself. This undoubtedly can have an unjustified but damaging effect on their confidence in their credit union.

Additionally, one of the residual effects that goes largely unnoticed is the impact that the reissuance of a card has on the neural network of a credit union. This is a credit union's own fraud detection system. Some of the components of the system are payment patterns and history of card usage, as is the case with most neural networks. Every time a credit union has to reissue a card, the pattern and history for that member is erased and it starts over. This increases the chance that the member will make a purchase that is perfectly acceptable, but get denied because the network does not recognize that what they are doing is perfectly normal. This is especially true for credit union members who travel.

Unfortunately, credit unions often never see any reimbursement for their costs associated with the majority of data breaches. Even when there are recoupment opportunities, such as the recent Target settlement with MasterCard, it is usually only pennies on the dollar in terms of the real costs and losses incurred. Meanwhile, big box retailers that were negligent in recent data security breaches are posting record profits. A 2015 Columbia University review of financial statements of merchants such as Target and Home Depot reveals that retailers barely notice a financial hit from massive data breaches, and breach costs were less than one-tenth of one percent of these giant retailers 2014 annual sales.

Payment networks are critical partners to credit unions in ensuring credit union members have the credit and debit card programs they need and demand. Collectively, the networks have worked together to standardize the Payment Card Industry (PCI) Data Security Standard designed to provide merchants and retailers with a framework of specifications, tools, measurements and support resources to ensure the safe handling of cardholder information. While NAFCU

appreciates the positive progress is this regard, credit unions and other issuers are still seeing steep losses in the wake of retailer and merchant data breaches and would like to see the networks do everything they can to make reimbursement in the wake of fraud stemming from a data breach more equitable. As discussed, NAFCU believes the negligent entity should be wholly responsible for such damages.

NAFCU's Key Data Security Principles

NAFCU has long been active on the data security front, and was the first financial services trade association to call for Congressional action in the wake of the 2013 data breach at Target. Recognizing that a legislative solution is a complex issue, NAFCU's Board of Directors has also established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **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 enact legislation 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.

Preventing Future Breaches

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.

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 *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 10 year study, 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 retailers and merchants, and therefore consumers, more vulnerable to breaches.

In addition, the report finds that the use of EMV cards ("chip 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. While some argued for the "chip card" solution, the reality is that it is not a panacea and does not replace a sound data security standard.

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 is the bipartisan legislation that was introduced in the 114th Congress by Senators Roy Blunt and Tom Carper and Congressman Randy Neugebauer. The legislation, S. 961/H.R. 2205, the *Data Security Act of 2015*, would have set a national data security standard that recognized those who already have one under the GLBA. We supported these bills and would urge for reintroduction in both the Senate and the House.

As the committee is aware, the cyber and data security discussions cross the jurisdiction of several Congressional committees. Given the daunting task of making meaningful reform in these areas, NAFCU would like to encourage congressional leadership to create a bipartisan and bicameral working group to find a legislative path forward to help better protect consumers from ongoing data breaches.

Conclusion

Cyber and data security, ensuring member safety, and how to incentivize and emphasize data safekeeping in every link of the payments chain is a top challenge facing the credit union industry today. Given the breadth and scope of many recent retailer and merchant data breaches, we have reached a tipping point in the public dialogue about how to tackle these issues. NAFCU member

credit unions and the 106 million credit union members across the country are looking to Congress to continue work on cyber and data security issues and move forward with legislation that will make a meaningful difference to consumers. It is time to level the playing field and require equal data security treatment to all those who collect and store personally identifiable and financial data.

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.

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