Testimony of

Debra Schwartz

President & CEO

Mission Federal Credit Union

on behalf of

The National Association of Federally-Insured Credit Unions

“Data Security: Vulnerabilities and Opportunities for Improvement"

Before the

House Financial Services Subcommittee on Financial Institutions and Consumer Credit

November 1, 2017

Introduction

Good morning Chairman Luetkemeyer, Ranking Member Clay and Members of the Subcommittee. Thank you for the invitation to appear before you this morning. My name is Debra Schwartz and I am testifying today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU). I am the President and CEO of Mission Federal Credit Union (Mission Fed), headquartered in San Diego, California, and also serve on NAFCU's Board of Directors as Treasurer.

Mission Fed is a federally charted credit union serving those who live, work or attend school in San Diego County. We serve more than 219,000 members through 30 local branches, making Mission Fed the largest locally-based credit union exclusively serving San Diego County.

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 110 million credit union members they represent that have been heavily impacted by ongoing data security breaches through no fault of their own.

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 data security front, the impacts of recent retailer and credit bureau data breaches on credit unions and consumers, including the financial

burdens they have faced. I will also outline 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 2016 as a year when "cyber attackers revealed new levels of ambition." According to the report, more than 1.1 billion identities were exposed in security breaches last year, which was nearly double the total from 2015. While large companies across all sectors are still a prime target for malware, the report notes that "small-to-medium sized businesses were the most impacted."

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.

NAFCU supports comprehensive data and cybersecurity measures to protect consumers' personal data. Credit unions and other depository institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA) and are examined by a regulator for compliance with these standards. Unfortunately, there is no comprehensive regulatory structure similar to what GLBA put in place for depository institutions for other

entities that may handle sensitive personal and financial data. Too often, credit unions are left cleaning up the mess and helping their members restore their personal financial information after another entity has suffered a breach. Enough is enough. Something must be done.

In today's digital economy, data security poses a threat to businesses of all sizes, individual consumers, and even national security. 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. Congress must require this.

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 and that is enforced to help prevent further breaches from occurring. Now is the time for Congress to act to create a national standard on data security for those who do not already have one.

Credit Unions and the *Gramm-Leach-Bliley Act*

GLBA and its implementing regulations have successfully limited data breaches among depository 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 depository institutions

such as credit unions. While credit reporting agencies, such as Equifax, are governed by some of the data security standards set forth by GLBA, they are not examined by a regulator for compliance with these standards in the same manner as depository institutions are under the act. This is an area that likely needs addressing.

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.

NAFCU believes the best way to move forward and prevent data breaches is to create a comprehensive framework for industries that are not already subject to data security standards of regulatory oversight with the responsibility to protect consumer data they collect and enforcing those standards. Entities that are considered "GLBA institutions" should be regularly examined by a regulatory body. The oversight of credit unions, banks and other depository 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 prudential 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 depository 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 credit union 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 credit union 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 credit union 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 data security measures, it should be noted that scalability is achievable and that it is inaccurate when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying sized 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 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 credit union 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.

A credit union 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 credit union 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. This is one area that Equifax appears to have failed in light of the recent breach. A regulator overseeing and examining their programs would have likely made sure that they had a timely notification plan in place.

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 Data Security

Since the passage of GLBA, 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 data security through periodic examinations designed to assess the risks associated with IT

environments of varying size and complexity. Currently, credit bureaus are not regularly examined for adherence to data security standards by a regulatory body.

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 data security 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.

Protecting Consumer Data is Important

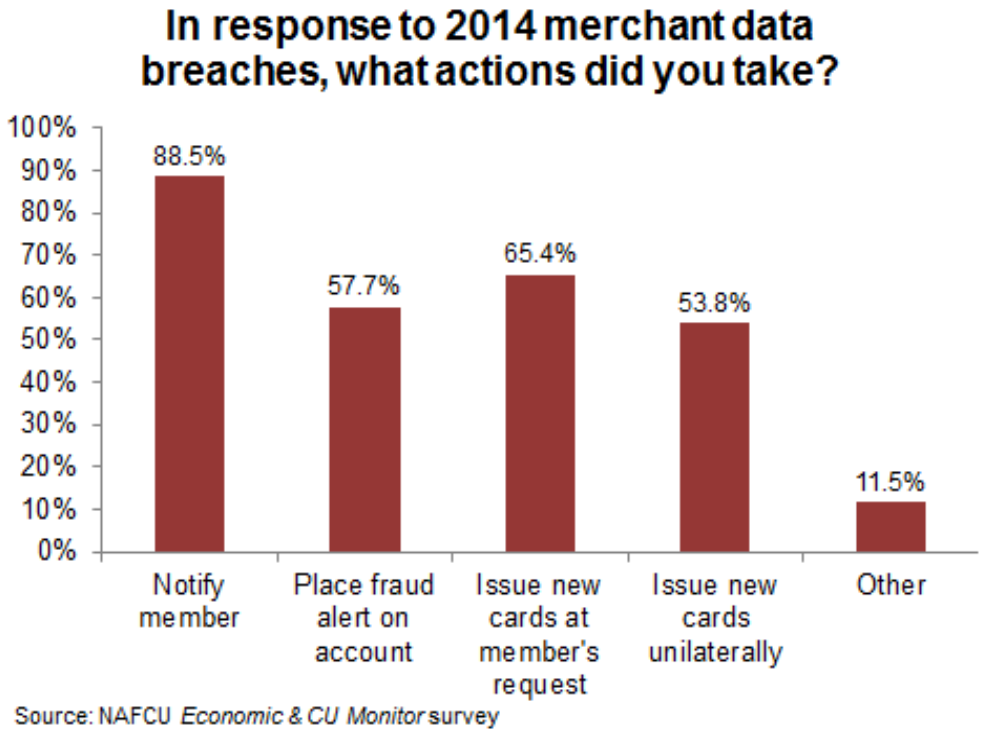
With the increase of massive data security breaches, from the Target breach at the height of holiday shopping in 2013 impacting over 110 million consumer records to the recent Equifax breach impacting up to 143 million consumers (43 percent of the U.S. population) Americans are becoming more aware and more concerned about data security and its impact. A recent Gallup poll found that 69 percent of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers, while a 2016 Gallup survey reported that 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.

Since the Target and Home Depot breaches, which brought large scale data breaches to light, there have been many others varying by industry, including the most recent Equifax and Yahoo breaches. Data security breaches are not just a retailer problem, but occur across many industries. This highlights the need for a comprehensive national data security standard to protect data akin to what is in place for depository institutions under GLBA.

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 data breach in 2014.

While the headline grabbing breaches are certainly noteworthy, the simple fact is that data breaches throughout our nation are happening almost every day. A survey of NAFCU member credit unions in June 2017, found that respondents were alerted to potential breaches an average of 189 times in 2016. Over 40 percent of the respondents said that they saw an increase in these alerts from 2015, while only 14 percent reported a decrease. When credit unions are alerted to breaches, they take action to 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.

Every entity collecting and storing consumers' personal and financial information regardless of industry are targets of cyberattacks. The difference, however, is that credit unions have been required to develop and maintain robust internal protections to combat these attacks and are

required by federal law and their regulator to protect this information as well as notify their members when a breach occurs that puts them at risk. As outlined above, 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. Entities that are considered "GLBA institutions" should be regularly examined by a regulatory body. This includes national credit bureaus such as Equifax, which are not currently examined.

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

1. Firewall (including redundant and internal firewalls)
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

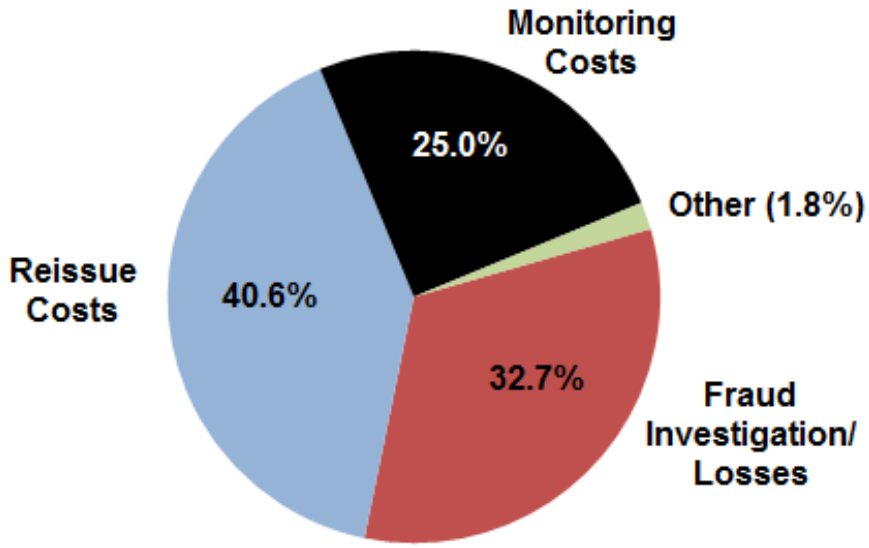
12. Encryption

13. End point security

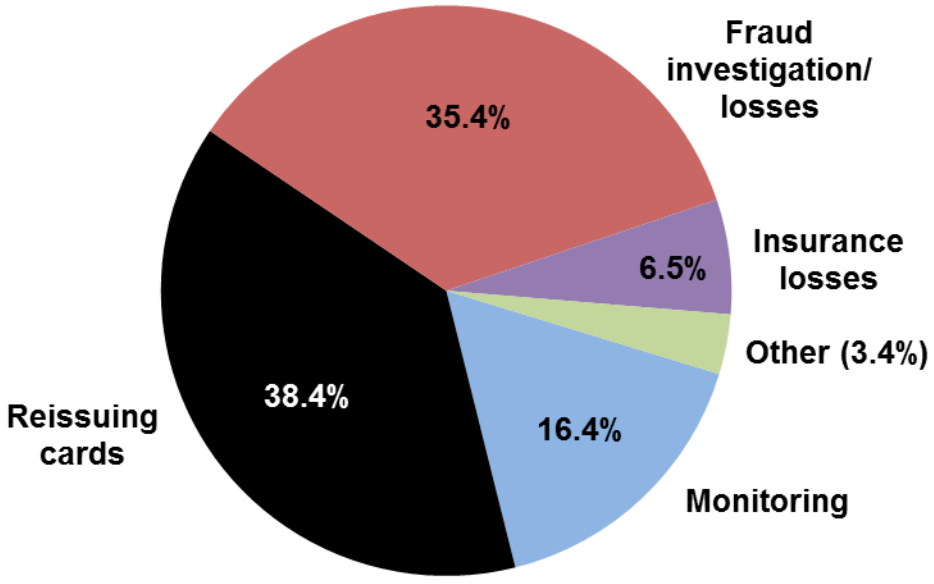
These elements can have a significant cost to the institution. A February, 2015, survey of NAFCU members found that the average respondent credit union spent $136,000 on data security measures in 2014, which does not even factor in the additional costs that the credit union faced due to data breaches at other entities. At Mission Fed, we have already spent over $1 million in 2017 to protect our members, including hardware and software updates for the encryption of data, and DDoS protection and testing. This does not even include internal staff costs.

The ramifications of recent data breaches for credit unions and their members have been monumental. The July 2017 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2016 were $362,000 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.

Percent of Fraud-Related Costs in 2014



Share of CU Fraud-Related Costs in 2016



Source: NAFCU *Economic CU Monitor* survey (July 2017)

Another cost, though difficult to measure, is that 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. I hear from many of my tellers that members sometimes question the credit union's security when their information is compromised. 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, those that were negligent in recent data security breaches are posting record profits. A 2015 Columbia University review of financial statements of

merchants reveals that retailers barely notice a financial hit from massive data breaches. At Mission Fed, we have seen over $1.7 million in card fraud already in 2017 and have incurred $6.3 million in card fraud since 2013. Because insurance costs have risen so high, we self-insure, so this is money that ultimately impacts our ability to make loans or provide programs to our members.

At Mission Fed, we participate in MasterCard's Account Data Compromise (ADC) Program which notifies us of events where our members' cards have been involved in a security breach. Since January 2013, we have received nearly 1,400 ADC notifications from MasterCard affecting our cardholders.

Mission Fed takes cardholder security seriously, so we choose to reissue new cards to members anytime a member's card appears on an ADC event notice. Since January 2013, we have reissued over 146,000 cards as a result of ADC notifications. To put that in perspective, we have approximately 280,000 cards issued to our members, so more than 50% have been replaced as a result of a compromise. This number does not include card replacements due to member reported fraud, as we always block cards involved in fraud reported by members.

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 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 depository institutions are required to meet certain criteria for safekeeping

consumers' personal information and are held accountable if that criteria is not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities 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 depository 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 those 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 negligent entity 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 entities 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 depository institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach. Once again, all "GLBA institutions," including credit bureaus, should be subjected to examinations by a regulatory body as depository institutions already are. Additionally, consumers whose personal and financial data has been compromised have a right to be notified in a timely manner. This is where Equifax failed by waiting weeks to notify the public, including credit unions, of their breach. Unfortunately, Equifax's silence left the door open for more damage to be done from fraud. Depository institutions servicing the accounts should be made aware of any breach at a national credit bureau as soon as practicable so they can proactively monitor affected accounts, and any notification requirements should be enforced by a regulator. Congress needs to act to make this happen.

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, <u>not one single company was in compliance with the PCI standards at the time of the breach.</u>

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. At Mission Fed, we have found that the EMV shift has done little to stem the increasing tide of fraud. 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 data and cyber 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 so far on the issue of data security is the bipartisan legislation that was introduced in the 114th Congress by Representatives Randy Neugebauer and John Carney. The legislation, 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 were pleased to see the bill get bipartisan support in this Committee in the last Congress and urge you to reintroduce and consider this legislation in this Congress.

As the committee is aware, the cyber and data security discussions cross the jurisdiction of several Congressional committees. The House Energy and Commerce Committee also advanced its own version of a data security bill in the last Congress. We would urge the Committee to

work with leaders on that Committee to craft a package that can get bipartisan support in both Committees. There have been industry discussions underway amongst interested groups and we would urge the Committee to work with industry to introduce and advance a package to create a robust national data security standard that can be enacted into law. The time for action is now.

We would also like to express our support for Title I of H.R. 4028, the *PROTECT Act of 2017,* offered by Representative McHenry, which would subject the credit bureaus to supervision and examination by the FFIEC. This would help address some of the concerns about the regulation of credit bureaus that I outlined earlier in my testimony. However, we believe other aspects of the bill, including Title III's phase-out of the credit bureau's use of Social Security Numbers, need further study for potential broader negative unintended impacts.

Conclusion

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 data breaches, we have reached a tipping point in the public dialogue about how to tackle these issues. NAFCU member credit unions and the 110 million credit union members across the country are looking to Congress to address data security issues and move forward with meaningful legislation that will make a 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 entities collecting and storing personal financial information 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.