

**PROTECTING CONSUMERS: FINANCIAL
DATA SECURITY IN THE AGE OF
COMPUTER HACKERS**

HEARING
BEFORE THE
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTEENTH CONGRESS
FIRST SESSION

—————
MAY 14, 2015
—————

Printed for the use of the Committee on Financial Services

Serial No. 114-23



U.S. GOVERNMENT PUBLISHING OFFICE

95-067 PDF

WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
PETER T. KING, New York	CAROLYN B. MALONEY, New York
EDWARD R. ROYCE, California	NYDIA M. VELÁZQUEZ, New York
FRANK D. LUCAS, Oklahoma	BRAD SHERMAN, California
SCOTT GARRETT, New Jersey	GREGORY W. MEEKS, New York
RANDY NEUGEBAUER, Texas	MICHAEL E. CAPUANO, Massachusetts
STEVAN PEARCE, New Mexico	RUBEN HINOJOSA, Texas
BILL POSEY, Florida	WM. LACY CLAY, Missouri
MICHAEL G. FITZPATRICK, Pennsylvania	STEPHEN F. LYNCH, Massachusetts
LYNN A. WESTMORELAND, Georgia	DAVID SCOTT, Georgia
BLAINE LUETKEMEYER, Missouri	AL GREEN, Texas
BILL HUIZENGA, Michigan	EMANUEL CLEAVER, Missouri
SEAN P. DUFFY, Wisconsin	GWEN MOORE, Wisconsin
ROBERT HURT, Virginia	KEITH ELLISON, Minnesota
STEVE STIVERS, Ohio	ED PERLMUTTER, Colorado
STEPHEN LEE FINCHER, Tennessee	JAMES A. HIMES, Connecticut
MARLIN A. STUTZMAN, Indiana	JOHN C. CARNEY, Jr., Delaware
MICK MULVANEY, South Carolina	TERRI A. SEWELL, Alabama
RANDY HULTGREN, Illinois	BILL FOSTER, Illinois
DENNIS A. ROSS, Florida	DANIEL T. KILDEE, Michigan
ROBERT PITTENGER, North Carolina	PATRICK MURPHY, Florida
ANN WAGNER, Missouri	JOHN K. DELANEY, Maryland
ANDY BARR, Kentucky	KYRSTEN SINEMA, Arizona
KEITH J. ROTHFUS, Pennsylvania	JOYCE BEATTY, Ohio
LUKE MESSER, Indiana	DENNY HECK, Washington
DAVID SCHWEIKERT, Arizona	JUAN VARGAS, California
FRANK GUINTA, New Hampshire	
SCOTT TIPTON, Colorado	
ROGER WILLIAMS, Texas	
BRUCE POLIQUIN, Maine	
MIA LOVE, Utah	
FRENCH HILL, Arkansas	

SHANNON MCGAHN, *Staff Director*
JAMES H. CLINGER, *Chief Counsel*

CONTENTS

	Page
Hearing held on:	
May 14, 2015	1
Appendix:	
May 14, 2015	63

WITNESSES

THURSDAY, MAY 14, 2015

Dodge, Brian A., Executive Vice President, Communications and Strategic Initiatives, the Retail Industry Leaders Association (RILA)	8
Moy, Laura, Senior Policy Counsel, New America's Open Technology Institute	13
Orfei, Stephen W., General Manager, PCI Security Standards Council	11
Oxman, Jason, Chief Executive Officer, the Electronic Transactions Association (ETA)	9
Pawlenty, Hon. Tim, President and Chief Executive Officer, the Financial Services Roundtable	6

APPENDIX

Prepared statements:	
Hinojosa, Hon. Ruben	64
Dodge, Brian A.	67
Moy, Laura W.	74
Orfei, Stephen W.	90
Oxman, Jason	96
Pawlenty, Hon. Tim	110

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Hensarling, Hon. Jeb:	
Written statement of the American Council of Life Insurers	120
Written statement of the National Association of Federal Credit Unions ..	121
Written statement of the National Association of Insurance Commissioners	123
Capuano, Hon. Michael:	
Written statement of the Office of the Attorney General of the Commonwealth of Massachusetts	132
Fincher, Hon. Stephen:	
Comments for the record submitted by the Secure ID Coalition	138
Foster, Hon. Bill:	
Written responses to questions for the record submitted to Jason Oxman .	141
Written responses to questions for the record submitted to Hon. Tim Pawlenty	142
Luetkemeyer, Hon. Blaine:	
Written statement of the Credit Union National Association	144
Stivers, Hon. Steve:	
Written statement of the National Retail Federation	149

**PROTECTING CONSUMERS: FINANCIAL
DATA SECURITY IN THE AGE OF
COMPUTER HACKERS**

Thursday, May 14, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The committee met, pursuant to notice, at 10:01 a.m., in room 2128, Rayburn House Office Building, Hon. Jeb Hensarling [chairman of the committee] presiding.

Members present: Representatives Hensarling, Royce, Lucas, Garrett, Neugebauer, Pearce, Posey, Fitzpatrick, Westmoreland, Luetkemeyer, Huizenga, Duffy, Hurt, Stivers, Fincher, Stutzman, Mulvaney, Hultgren, Ross, Pittenger, Barr, Rothfus, Messer, Schweikert, Guinta, Tipton, Williams, Poliquin, Love, Hill; Waters, Maloney, Sherman, Meeks, Capuano, Hinojosa, Clay, Lynch, Scott, Green, Cleaver, Moore, Ellison, Perlmutter, Himes, Carney, Sewell, Kildee, Murphy, Delaney, Beatty, and Vargas.

Chairman HENSARLING. The Financial Services Committee will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time.

Today's hearing is entitled, "Protecting Consumers: Financial Data Security in the Age of Computer Hackers."

Members, welcome home. I assume many of our colleagues are furiously running here from HVC-210 as we speak. For our witnesses and for the audience, we have been nomads since the beginning of the year.

So you will notice a few changes in the room. This renovation was caused by an upgrade of the audiovisual systems. Although I did not specifically request it, I now notice there are twice as many microphones in our hearing room as before. I wish to notify Members that that does not mean they can speak for twice as long. That doesn't go along with the microphones.

In addition, you will notice that our witnesses are quite a ways away, and that we have less room for the public. As hearing rooms are renovated, they must be made and should be made compliant with the Americans with Disabilities Act (ADA). This room complies with the ADA statute, which means that every row has been enlarged. This means that we have lost part of our gallery, but the overflow room is still alive and well.

In addition, for those who have ever moved into a new home or new apartment, there is such a thing known as a "punch list." And

so, for some of the subcommittees, you may be kicked out of this room over the next 5 to 7 days as that punch list is completed.

Another change in our committee room: If you will look over my left shoulder, you will see the portrait of our most recent chairman, Spencer Bachus. For those who have some tenure on the committee, including myself and the ranking member, to have Barney over one shoulder and Spencer over the other kind of seems like old times.

We certainly know of Barney's fierce intellect and tenacity, but I also hope that Members will remember Spencer's gentle and kind leadership of this committee. And sometimes when emotions and passions start to run high, let's remember the example he set for us with respect and decency and, yes, humor.

Somehow, at any moment, I expect these two to carry on one of their classic debates. We will see if that actually happens or not.

I believe that is all I need to say about the hearing room at the moment, in which case the Chair now recognizes himself for 3 minutes for an opening statement.

At today's hearing, we will be focused on protecting consumers and their private financial information in an age of computer hackers.

The world has experienced a technology revolution, one that has brought remarkable benefits to consumers and the broader economy, but has also increased risks on consumers by making the theft of personal financial information a profitable enterprise for cyber criminals and computer hackers.

In the era of big data, large-scale security breaches are unfortunately all too common. And every breach leaves consumers exposed and vulnerable to identity theft, fraud, and a host of other crimes. We have certainly all read about the high-profile, headline-grabbing breaches at Target and Home Depot. According to the Identity Theft Resource Center, there were 783 U.S. data breaches in 2014, an increase of more than 27 percent over the prior year. The Center for Strategic and International Studies and McAfee Security estimate that such attacks cost the U.S. economy \$100 billion—that is "billion" with a "B"—annually.

American consumers rightfully expect their personal information to be protected by their financial institutions, and by retailers, card networks, payment processors, and, yes, their Federal Government. Consumers shouldn't be left to simply hope and pray their personal information will be safe every time they swipe their debit or credit card or enter their information online. They deserve protection.

So today the committee will hear from representatives of organizations whose members constitute the major participants in the payment system. We welcome their expertise and insight.

My hope is that this hearing affords Members on both sides of the aisle an opportunity to better understand what security measures are currently in place to prevent data breaches, how consumers are notified following a breach, what types of emerging technologies will help reduce the frequency and severity of breaches, what steps are being taken by the merchants and financial services communities to address the problem, and where additional Federal legislation may be warranted.

I further hope that the committee will engage in a thoughtful and constructive dialogue on a bipartisan basis. And, in that regard, I wish to thank Chairman Neugebauer and the gentleman from Delaware, Mr. Carney, for starting this bipartisan dialogue off on the right foot by introducing a bipartisan bill to address this important problem.

I will now yield back the balance of my time and recognize the ranking member for 3 minutes.

Ms. WATERS. Thank you, Mr. Chairman.

Americans are increasingly reliant on electronic means to communicate, shop, and manage their finances. While new technologies bring substantial opportunity, they also bring a range of new vulnerabilities for consumers. Massive attacks on some of our Nation's largest retailers and financial institutions are impacting virtually every sector of our economy and our national security.

Consumers are not the only ones who pay the price of a breach. The cost of recovering losses by retailers and card issuers can be extensive and weigh particularly heavy on small community banks and credit unions.

We all know companies face a number of challenges in determining how best to secure customers' financial and personally identifiable information. In addition, we know that there are significant costs to complying with various State laws and providing notice after a breach.

However, as we consider setting national standards for safeguarding consumers' personal information and ensuring timely notification, we must again acknowledge the good work of those States that for years have been at the front lines of this fight. I believe that any Federal preemption should complement States' protections and ensure at a minimum that State attorneys general continue to play an important role in enforcement and notification standards.

In setting minimum standards, we need to be careful not to hamstring our State and Federal regulators' ability to continue adapting and strengthening protections for consumers. Otherwise, we will limit regulators' ability to keep up with technological change.

And we must preserve a private right of action for consumers and for financial institutions to ensure that affected entities and breach victims have legal recourse.

Further, consumers must be consistently provided with clear disclosures of the rights and remedies available to them so that they remain aware of the various ways in which they can protect themselves from identity theft, fraud, and other cyber crimes.

Mr. Chairman, efforts to guard against cyber threats are critically important and shouldn't devolve into the same partisan fault lines we have seen on far too many other issues before this committee, such as the baseless attacks on watchdogs like the CFPB, and blocking efforts to reauthorize the charter of the Export-Import Bank, which expires in just 22 legislative days.

With that, I look forward to hearing from the witnesses today, and I yield back the balance of my time.

Chairman HENSARLING. The gentlelady yields back.

The Chair now recognizes the gentleman from Texas, Mr. Neugebauer, chairman of our Financial Institutions Subcommittee.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

We live in a world where the global marketplace is supported by a global payments system. It delivers payment services to consumers in the blink of an eye. Immense amounts of sensitive consumer information is transferred and processed and stored in any one transaction.

The security of the system is only as strong as its weakest link, and today I look forward to learning more about new payment technologies that continue to facilitate payment efficiency, speed, and security. I am hopeful we can have a robust policy discussion about what new data security standards are needed to level the playing field.

This month, Congressman Carney and I introduced bipartisan legislation which builds on the work of Senators Carper and Blunt. Our starting point was to look at Gramm-Leach-Bliley, which laid out a robust data security framework for financial institutions. Almost 16 years later, this framework has worked very well.

The data security standards in H.R. 2205 are based on certain core principles.

First, because we have a global payment system, we need a national data security standard and a national breach notification standard. This standard must minimize regulatory requirements but must carry with it a strong Federal enforcement mechanism.

Second, the data security standard must be technology-neutral and process-specific. It must reasonably identify certain core elements in the absence of an FTC rulemaking.

Third, it is absolutely necessary that the data security standard is scalable based on the size of the business, the scope of the operation, and the type of information that it holds. Legislation must recognize that the corner market cannot and should not have the same standard as the largest retailer operating in 50 States.

While I am confident in our bipartisan legislation, I am open to working with any member of the interested groups to minimize unintended consequences and to continue tailoring this legislation. We have a shared interest in seeing this legislation signed into law, giving consumers the safest payment system possible.

And with that, I want to thank our panel for being here this morning. Based on my review of the testimony that has been submitted, I think this is going to be very informative for our Members. And I think it is good that we have these different interests at the table today.

And so, Mr. Chairman, I look forward to a very informative hearing.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Delaware, Mr. Carney, for 2 minutes.

Mr. CARNEY. Thank you, Mr. Chairman.

Mr. Chairman, over the last decade alone, data breaches have compromised nearly a billion records containing sensitive consumer financial information. Experts estimate that when a data breach occurs in the United States, it directly costs consumers an average of \$290 per victim. Studies show that cyber criminals are costing U.S. companies approximately \$100 billion a year.

One thing is clear: The current patchwork of 47 different State data breach laws is failing to protect American consumers. That is why Mr. Neugebauer and I have worked together on a bipartisan effort to develop a data security and breach notification framework within which all relevant stakeholders can operate. We think consumers and the companies that handle their personal financial data should all know the rules of the road when it comes to the standard for protecting this data.

Our bill, H.R. 2205, the Data Security Act, builds off the efforts by Senators Carper and Blunt across the Capitol. The bill implements a strong national data breach notification standard. It requires companies to enact a data security program that is robust and scalable and with the goal of protecting consumers' personal information from breaches. And it sets reasonable standards for accurate and timely notice to consumers when a breach occurs.

Importantly, the bill's requirements avoid a one-size-fits-all approach and allow companies of varying sizes and complexity to find a program that is tailored and effective for their business.

As with any comprehensive piece of legislation, our bill can always be improved. The example clarifying that the preemption provision does not have unintended consequences outside the issues covered in this bill merits further attention. I am looking forward to working with my colleagues on both sides of the aisle to make improvements to this legislation where necessary.

The fact is, though, that the White House, Congress, and the private sector and consumers all agree that the status quo is not acceptable. And I am encouraged that this committee is having this hearing today and that we are moving forward to protect consumers, businesses, and the American economy.

I would like to thank Mr. Neugebauer for his leadership on this issue, and I look forward to hearing the witnesses' testimony and feedback in this hearing.

Thank you. I yield back.

Chairman HENSARLING. The gentleman yields back.

And, indeed, it is time to hear from our witnesses. We welcome each and every one of them to the panel.

The Honorable Tim Pawlenty is the president and chief executive officer of The Financial Services Roundtable, and a former Governor of the State of Minnesota.

Mr. Brian Dodge is the executive vice president of communications and strategic initiatives at the Retail Industry Leaders Association.

Mr. Jason Oxman is the chief executive officer of the Electronic Transactions Association.

Mr. Stephen Orfei is the general manager at PCI Security Standards Council.

And last but not least, Ms. Laura Moy is a senior policy counsel at New America's Open Technology Institute.

Several of you have testified before Congress before; I am not certain about all of you. So we have a rather simple lighting system. Green means go. Yellow means hurry up because the red light is soon to follow. And red means stop. The yellow light comes on with 1 minute to go.

Each of you will be recognized for 5 minutes to give an oral presentation of your testimony. And without objection, each of your written statements will be made a part of the record.

And since we are brand-new in our refurbished space—in the old hearing room, you had to pull these microphones very close to you. I think now you can keep them a somewhat comfortable distance from your mouth.

Governor Pawlenty, you are about to be our guinea pig on the new sound system. And, Governor Pawlenty, you are now recognized for your testimony.

**STATEMENT OF THE HONORABLE TIM PAWLENTY, PRESIDENT
AND CHIEF EXECUTIVE OFFICER, THE FINANCIAL SERVICES
ROUNDTABLE**

Mr. PAWLENTY. Good morning, Chairman Hensarling, Ranking Member Waters, and members of the committee. Thank you for the opportunity to share a few thoughts with you this morning about one of the most pressing issues facing our country, and that is the emerging, growing, and exponentially threatening cyber warfare that is taking place both commercially and otherwise across the globe and being visited upon American businesses and consumers in ways that I think deserve the Congress' attention.

Just to give you a sense of a few measures of what we are up against in this regard, 80 percent of the companies that were breached in 2014 did not know they were breached until somebody else told them, a third party told them—sometimes the government, sometimes a vendor, but a third party. And the average length of time between the breach actually happening and the discovery was months after the fact.

In addition, here is another interesting fact. Over half of the adult American population had their personal data exposed last year, according to a CNN published report.

And the list goes on, including that we now know through public and confirmed reports that this is no longer college kids in their basements having some fun trying to get into some systems. These are nation-state actors, including—or semi-state-nation actors, including China, North Korea, Iran, Russia, and former Soviet Union-sponsored states and individuals and enterprises associated with them, and very sophisticated international crime syndicates.

If one of those entities triangulates on a company, it is likely not going to end well for that company or their customers. So we need a more robust, more muscular response to these threats. And we appreciate very much the fact that this committee is paying attention to these issues.

And, Mr. Chairman, thank you to the House for passing on more than one occasion threat information legislation, CISA and CISPA legislation. We hope the Senate does the same. And, again, we are not talking about sharing personal information, but that threat-information-sharing bill is very helpful to this cause and making the country more prepared to defend against these threats.

As it relates to the financial services sector and the payment system, our sector, as the chairman mentioned, has been dealing with these issues in a regulated context for quite some time. The Gramm-Leach-Bliley Act passed in 1999. Part of that Act, of

course, was to visit upon this industry data security standards and enforcement mechanisms, including part of the examination process.

That, I think, has served the industry well. As you look at the percent of breaches that have taken place in recent years, our sector has the lowest breach incident rate. We still have a lot of work to do, but compared to other major sectors, that is progress. And that is because of some of the good work that has been done since Gramm-Leach-Bliley and otherwise.

We are about to launch some more secure top-level domains, dot-bank and dot-insurance, which should help with these issues. We have been involved in an information sharing and analysis center, one of the first in the country that is most robust, the FS-ISAC, and more.

As it relates to the payment system, it is about to get a lot better. We are going to move, as a next step, to the chip-enabled cards. It is already happening. The networks have said, look, if you want to avoid fraud liability, you have to make this transition towards the end of 2015. There are some saying, "Look, we are not ready. It is going to take a little longer." But over the course of the next couple of years, almost all cards are going to be chip cards, and that is going to help.

But don't be focused just on that. That is technology from the 1960s. Magnetic strips were invented in the 1960s. PINs were invented in the 1960s; chips, of course, more recently. But it is moving well beyond that discussion. The new technologies that are coming forward and being actively considered include voice recognition, facial recognition, biometrics, location confirmation, gesture recognition, and a lot more. So this space is evolving extremely rapidly and is going to continue to evolve as new technology emerges.

As to the legislation that is before you, Congressman Neugebauer, Congressman Carney, thank you very much. We strongly support H.R. 2205. We think it is an excellent piece of work. May need some modifications, as Congressman Carney mentioned, but it does some important things.

It creates for all sectors, not just the healthcare sector or the financial services sector, a data security standard, which is really important. And it is flexible. We are only as strong as the weakest link in the chain. If we have strong standards but one of the other links in the chain doesn't, the whole system is exposed. So thank you for putting the marker down on a strong national data security standard. We strongly support that.

Another important piece of the bill is a uniform data breach notification law. Many States, including my own, have strong laws in this regard, but as you think about cyberspace and how commerce gets conducted now, it doesn't make a lot of sense to have 50 different standards, 50 different approaches, 50 different responses to a breach and the notification relating to it.

And, in closing, as you think about this, we are not asking for any current State initiatives to be diluted. We think, if you set a standard, set it high. Make it nation-leading.

And I am out of time. Mr. Chairman, again, thank you for the chance to be here this morning. Thank you to Congressmen Neuge-

bauer and Carney for their leadership on these issues. We strongly support what you are trying to do.

[The prepared statement of Mr. Pawlenty can be found on page 110 of the appendix.]

Chairman HENSARLING. Thank you, Governor.

Mr. Dodge, you are now recognized for 5 minutes for your testimony.

STATEMENT OF BRIAN A. DODGE, EXECUTIVE VICE PRESIDENT, COMMUNICATIONS AND STRATEGIC INITIATIVES, THE RETAIL INDUSTRY LEADERS ASSOCIATION (RILA)

Mr. DODGE. Thank you, and good morning.

Chairman Hensarling, Ranking Member Waters, and members of the committee, my name is Brian Dodge, and I am an executive vice president with the Retail Industry Leaders Association. Thank you for the opportunity to testify today about data security and the steps the retail industry is taking on this important issue and to protect consumers.

RILA is the trade association of the world's largest and most innovative retail companies. Retailers embrace innovative technology to provide American consumers with unparalleled services and products. While technology presents great opportunities, nation-states, criminal organizations, and other bad actors are also using it to attack businesses, institutions, and governments.

As we have seen, no organization is immune from attacks. Retailers understand that defense against cyber attacks must be an ongoing effort. As leaders in the retail community, we are taking new and significant steps to enhance cybersecurity throughout the industry.

To that end, last year RILA formed the Retail Cyber Intelligence Sharing Center, or R-CISC, in partnership with America's most recognized retailers. The Center has opened a steady flow of information-sharing between retailers, law enforcement, and other relevant stakeholders.

Also, the R-CISC has recently established a formal working relationship with the Financial Services ISAC, a move that will, among other things, ensure collaboration across the payments ecosystem on these issues.

RILA applauds the House for passing cyber information-sharing legislation, and we hope the Senate will quickly take up and adopt H.R. 1560's flexible approach to electronic sharing.

While I expect we will discuss many cybersecurity topics today, one area of security that needs immediate attention is payment card technology. The woefully outdated magnetic stripe technology used on cards today is the chief vulnerability in the payments ecosystem. Retailers are estimated to be investing more than \$8.6 billion to upgrade card terminals to accept chip cards by later this year. However, the new cards will not be issued with PINs.

Chip and PIN technology has proven to dramatically reduce fraud when it has been deployed elsewhere around the world. In contrast, chip and signature technology falls short of providing American consumers the best security available today.

Retailers believe that the two-factor authentication enabled through chip and PIN will prevent criminals from duplicating cards

with ease and devalue the data that retailers collect at the point of sale. Ultimately, these steps have been proven to substantially reduce the economic incentive for cyber criminals to launch these kinds of cyber attacks.

Before I discuss what RILA believes are important data breach policy considerations, I will briefly highlight the significant data security and data breach notification laws with which retailers currently comply.

Forty-seven States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have adopted data breach notification laws. In addition, retailers are subject to robust data security regulatory regimes. The Federal Trade Commission has prosecuted more than 50 cases against businesses that it charged with failing to maintain reasonable data security practices. These actions have created a common law of consent decrees that clearly spell out the data security standards expected of businesses.

Additionally, inadequate data security measures for personal information can lead to violations of express State data security laws. Also, many States have so-called “little FTC acts” that can be used to enforce against what attorneys general deem to be unreasonable data security practices.

Finally, retailers voluntarily and by contract follow a variety of security standards, including those maintained by PCI, NIST, and ISO.

While retailers diligently comply with this range of data breach notice and data requirements, a carefully crafted Federal data breach law can clear up regulatory confusion and better protect and notify customers. RILA supports Federal data breach legislation that is practical and proportional and sets a single national standard.

RILA supports data breach legislation that creates a single national notification standard that allows businesses to focus on quickly providing affected individuals with actionable information; that ensures that targeted notice is required only when there is an actual risk of identity theft, economic loss, or harm; that ensures that the responsibility to notice is that of the entity breached but provides flexibility for entities to contractually determine the notifying party; that establishes a precise and targeted definition for “personal information;” and that recognizes that retailers already have robust data security obligations and that security must be able to adapt over time.

I thank the committee for inviting me today, and I look forward to answering your questions.

[The prepared statement of Mr. Dodge can be found on page 67 of the appendix.]

Chairman HENSARLING. Mr. Oxman, you are now recognized for 5 minutes for your testimony.

**STATEMENT OF JASON OXMAN, CHIEF EXECUTIVE OFFICER,
THE ELECTRONIC TRANSACTIONS ASSOCIATION (ETA)**

Mr. OXMAN. Thank you, Mr. Chairman, Ranking Member Waters, and members of the committee for the opportunity to be here today.

I am Jason Oxman, the CEO of the Electronic Transactions Association. ETA is the trade association of the payments industry. Our more than 500 member companies are focused on providing the world's most secure, reliable, and functional payment systems to American merchants and consumers.

Electronic payments in the United States are largely invisible to consumers because, simply put, they just work. U.S. consumers carry 1.2 billion credit, debit, and prepaid cards in their wallets, and they can use those cards to pay electronically at more than 8 million merchants in the United States. Indeed, ETA member companies process more than \$5 trillion in U.S. consumer spending every year. That means thousands of transactions are moving across our network every second.

Now, consumers enjoy a wide variety of ways to pay electronically, including in person, with a card or a mobile device or a watch, or remotely via phone or over the Internet. And from the moment that a consumer initiates a payment, the transaction is securely transmitted, authorized, and processed within a matter of seconds. ETA member companies take very seriously the obligation to protect the security of their customers' information.

Consumers in the United States choose electronic payments because they benefit from zero liability for fraud, making electronic payments the safest and most secure way to pay. Today, criminal fraud amounts to less than 6 cents of every \$100 processed in transactions. It is a fraction of a tenth of 1 percent.

Now, even though fraud represents a tiny percentage of overall transaction volume, we are deploying cutting-edge new technology and using self-regulatory industry guidelines to bolster the fight against fraud. I would like to highlight three concrete steps our industry is taking to protect consumer information and prevent data breach.

First, ETA members are deploying EMV-enabled chip cards to fight the number one cause of card fraud: counterfeit cards. Counterfeit cards represent about two-thirds of card-present fraud in the United States today. Chip cards prevent cards from being counterfeited. They don't stop data breaches, but they do make it harder for criminals to reap the rewards of those data breaches.

Chip migration happening now in the United States is the most complicated overhaul of our payments technology system in the 40 years since the magnetic stripe card was introduced. Our banks need to replace more than 1 billion cards. Merchants need to upgrade point-of-sale equipment at more than 10 million locations. But we are working together, and we are getting it done.

Second, our industry is deploying new tokenization technology that replaces card information with a one-time-use token. Even if intercepted by criminals, these tokens cannot be used to generate fraudulent transactions. Think of a token as a mathematical cryptogram that can't be reproduced.

One well-known implementation of tokenization is in mobile payments, where the customer's phone or watch generates that token for use. Tokens can also be used in card environments, as well. And we are working with our merchant partners to deploy tokenization technology at both brick-and-mortar and online retail.

Third, ETA members are helping merchants secure the point of sale by deploying new encryption technologies. Point-to-point encryption is a way to secure all entry points against an attack. It denies cyber criminals the access they need to install malware and other cyber hacking tools.

As our industry deploys all of these layered technologies, I also want to affirm ETA's strong support for legislation that creates uniform national data standards and data protection breach standards as well. Such standards must be industry-neutral, and they must be preemptive of State law. And this is the approach set out in H.R. 2205, which ETA strongly supports. We applaud Chairman Neugebauer and Mr. Carney for engaging in this important dialogue with this legislation.

ETA also supports legislation to promote information-sharing. Sharing of information across government and across technology and manufacturing companies will support prevention of and investigation of breaches and ensure against cyber attacks.

Cyber criminals are increasingly sophisticated, they are global in scope, and we are working proactively to address every threat. We must not forget that these data breaches of merchants and consumers make them victims of crime. We share a desire to stamp out fraud, and we take seriously our responsibility to all of our customers to do so.

Thank you for the opportunity to be here, and I look forward to your questions, Mr. Chairman.

[The prepared statement of Mr. Oxman can be found on page 96 of the appendix.]

Chairman HENSARLING. Mr. Orfei, you are now recognized for your testimony.

STATEMENT OF STEPHEN W. ORFEI, GENERAL MANAGER, PCI SECURITY STANDARDS COUNCIL

Mr. ORFEI. Thank you, Mr. Chairman.

Good morning. My name is Steven Orfei. I am the general manager of the PCI Security Standards Council. I have the privilege of leading a talented and deeply committed membership organization that is responsible for the developing and maintaining of the global data security standards for the payment card industry.

Our approach combines people, process, and technology. Continuous effort in applying our standards is the best line of defense against organized crime, state-funded actors, and criminals who threaten our way of life and attempt to undermine our confidence in the financial system. Everyone has been victimized by these criminals, and we know the very real harm caused by breaches.

Developing standards to protect payment card data is something the private sector and specifically PCI is uniquely qualified to do. Consumers are understandably upset when their payment card data is put at risk. The Council was created to proactively protect consumers' payment card data.

Our community of over 1,000 of the world's leading businesses is tackling data security challenges, from simple issues—for example, the word "password" is still one of the most commonly used passwords—to complex issues like encryption.

Our standards are a solid foundation for a multilayered security approach. We aim to remove payment card data if it is no longer needed. Simply put, if you don't need it, don't store it. If it is needed, then protect it, and reduce the incentives for criminals to steal it.

And here is how we do that. The data security standard is built on 12 principles, covering everything from logical to physical security and much more. It is updated regularly through feedback from our global community. We manage eight other standards that cover card production, PIN-entry devices, payment applications, and much, much more. We work on technologies, best practices, and provide market guidance. We have laboratories to vet solutions that we list on our Web site. All of our information is free. Our mission is to educate, empower, and protect.

Now, our end-game strategy is to devalue the data so that it is useless in the hands of the bad guys. We have three technologies that will allow us to do so: EMV at the point of sale; point-to-point encryption; and tokenization. When bundled and implemented properly, the data becomes useless; then there is no reason to break in.

That is why the Council supports adoption of the EMV in the United States through organizations such as the EMV Migration Forum, and our standards support EMV today in other worldwide markets.

But EMV chip is not a silver bullet. Additional controls are needed to protect the integrity of payments online and in other channels. This includes encryption, tamper-resistant devices, malware protection, network monitoring, and more. All are vital parts of the PCI standards.

Effective security requires more than just standards, for standards without supporting programs are just tools, not solutions. The Council's training and certification programs have educated tens of thousands of security professionals and make it easier for businesses to choose products that have been lab-tested, certified as secured.

Finally, we conduct global campaigns to raise awareness of payment card security.

The committee's leadership on this critical issue is important, and there are clear ways in which the Federal Government can help—for example, by leading stronger cooperative law enforcement efforts worldwide, by encouraging stiff penalties for these crimes, and recent initiatives on information-sharing are also proving to be invaluable.

The Council is an active collaborator with government. We work with NIST, DHS, Treasury, the Secret Service, and many other government entities, including global law enforcement such as Interpol and Europol.

In conclusion, payment card security is complex. Silver-bullet solutions do not exist. Unilateral action is usually a disappointment. Alliances, partnerships, information-sharing, and collaboration between the public and private sector is critical.

The PCI Council stands ready and willing to do more to combat global cyber crimes that threaten our way of life and confidence in the financial systems of the world. We thank the committee for

taking a leadership role and seeking solutions to one of the largest security concerns of our time.

Thank you.

[The prepared statement of Mr. Orfei can be found on page 90 of the appendix.]

Chairman HENSARLING. Thank you.

And Ms. Moy, you are now recognized for your testimony.

STATEMENT OF LAURA MOY, SENIOR POLICY COUNSEL, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Ms. MOY. Thank you. Thank you so much, Chairman Hensarling. And thank you, Ranking Member Waters, and members of the committee. Thank you so much for your commitment to addressing data security and data breaches and for the opportunity to testify on this important issue.

Consumers today share tremendous amounts of information about themselves. Consumers benefit from sharing information, but they can be harmed if that information is compromised.

For the most part, the States are actively dealing with this issue in ways tailored to address the needs of their own residents but with a large body of common elements. At least 29 States have introduced or are considering breach notification bills or resolutions this year alone. Bills in 27 of those States would amend existing laws to account for changing needs and changing threats.

Only three States have no breach notification law on the books, and two of those States have considered bills this year to change that.

Consumers would therefore be best served by a Federal bill on this subject that sets a floor for disparate State laws, not a ceiling. But to the extent Congress seriously considers broad preemption, any new Federal standards should strengthen or at least preserve important protections that consumers currently enjoy at both the State and Federal levels.

Because any broadly preemptive Federal bill would bring an end to the rich legislative activity on the issue taking place in State legislatures, it would also need to provide a similarly agile mechanism for quickly adjusting the law in the future to match developing technology and new threats.

Unfortunately, a number of recent legislative proposals would actually diminish consumer protections in a number of ways by replacing strong and broad State protections with a weaker Federal standard. In addition, a number of the bills do not provide the flexibility we need to make sure consumers' personal information remains protected as the information landscape changes.

Don't get me wrong. Most of the bills we have seen would certainly offer some new benefits for consumers, but many consumer and privacy advocates, myself included, question whether those new benefits outweigh the potential harm to State jurisdictions and to consumers' existing protections.

I will therefore focus today on four potential shortcomings of Federal legislation that would need to be addressed in order to ensure that any new bill represents a net gain for all consumers.

First, Federal legislation should not ignore the serious physical, emotional, and other nonfinancial harms that consumers could suf-

fer as a result of misuses of their personal information. A bill that would both preempt State laws and condition breach notification on demonstrated risk of financial harm could actually reduce consumer protections in 33 States and the District of Columbia, where the existing law either has no harm trigger or has one that is not limited to financial harm.

Second, Federal legislation should not eliminate data security and breach notification protections for types of data that are currently protected under State or Federal law. Some current legislative proposals feature a narrow class of protected information along with broad preemption. Such legislation would eliminate protections consumers currently rely on at the State and sometimes Federal level. For example, many bills would eliminate protections in 10 States for health information or eliminate Federal protections for telecommunications, cable, and satellite records.

Third, Federal legislation should provide a means to expand the range of information covered by the bill as technology develops. The 10 State breach notification laws that now cover health information represent a clear trend, as States are currently updating existing consumer protections to respond to the growing threat of medical identity theft.

We can't always forecast the next big threat years in advance, but, unfortunately, we know that there will be one. Federal legislation on this topic must provide flexibility to meet new threats, whether by continuing to allow States to protect classes of information that fall outside the four corners of the bill or by establishing agency rulemaking authority on the definition of "personal information."

Fourth, and finally, Federal legislation should include enforcement authority for State attorneys general. Thousands of data breaches are reported each year, many of which affect only a small number of consumers. Federal agencies are well-equipped to address large data security and breach notification cases, but they could be overwhelmed if they lose the complementary support of State AGs, especially when it comes to handling smaller cases, providing guidance to small businesses, and providing resources for local consumers.

I and many of my fellow privacy stakeholders are not unequivocally opposed to the idea of Federal data security and breach notification legislation, but any such legislation must strike a careful balance between preempting existing laws and providing consumers with new protections. The Open Technology Institute therefore appreciates your close examination of this issue, and I am looking forward to your questions.

Thank you.

[The prepared statement of Ms. Moy can be found on page 74 of the appendix.]

Chairman HENSARLING. The Chair now yields himself 5 minutes for questioning.

So, based on my unofficial survey of the good folks in the Fifth District of Texas, whom I have the privilege of representing, data breach, although they don't typically use that phrase, certainly make their top 20 anxiety list and probably their top 10 when they think of identity theft, other forms of theft, or privacy loss.

So it is a very serious matter, but, as Ms. Moy was positing in her testimony, there is a cost and a benefit associated with anything we do around here. To state the obvious, we are lawmakers. And there was a law made about 15 years ago, Gramm-Leach-Bliley, that dictated standards. There has been a lot of innovation since Gramm-Leach-Bliley was written into law.

Let's start with you, Governor Pawlenty. What exactly is broken? What needs fixing here? Where does Gramm-Leach-Bliley work? Where doesn't it work?

Mr. PAWLENTY. Mr. Chairman, thank you. It is a great question.

If you just step back from how individuals might characterize it and ask them this question: How is the current system working? Half of the adult American population has their personal data exposed in one year. It is not a stretch of the imagination to think somebody could get into the electrical grid and shut it down in a big part of the country, not for a day but for a month or months on end. You do that, and you lose electricity in your district, lose pressure for natural gas pipelines, points of sales go down, you can't transact anything electronically. You have a very—not existential but very dramatic impact on the country.

So it requires, I think, a sense of urgency and a sense of understanding regarding the magnitude of the threat.

As to Gramm-Leach-Bliley, it works. It is flexible; it makes accommodations for the size of the business. But it says, given the importance of this infrastructure to the country, if the payment system doesn't work, if it is stalled or people lose confidence in it, you are going to have a big piece of the economy grind to a halt.

There are trillions of dollars of payments that flow through the northeastern United States per day. If that gets shut down or disrupted or interrupted, you have a material, I would say bordering on existential, threat to the economy of the country.

So this is an urgent deal. It is growing in terms of its concern exponentially. Gramm-Leach-Bliley works. However, no institution is immune. We have some of our biggest institutions that have been breached. The best in the world, the NSA, by everybody, 10 out of 10 in terms of world-class capabilities in this regard, breached by an insider threat.

So there is much more work to be done on all fronts. And we are the best of class. Financial services gets breached from time. We manage it. People get their money back. It is convenient. But the other sectors that don't have these kind of standards and capabilities need to up their game, and you can help lead that effort.

Chairman HENSARLING. Mr. Oxman, you, in your testimony, I think, were lauding the elements of the legislation by Mr. Neugebauer and Mr. Carney, about preemption and national standards. It seems to be an open question in Ms. Moy's mind regarding preemption and perhaps national standards. So why do you consider preemption and national standards to be so important?

Mr. OXMAN. Mr. Chairman, as a number of witnesses noted, we all share an interest in ensuring that consumers and merchants are protected. But when something does go wrong, we also need to make sure that we get the word out as quickly and efficiently as possible and make sure those protections that are available under law kick in.

The reason consumers use electronic payments is because they are 100 percent protected against any liability for fraud, but we still need to get information out to them.

There are 47 different regimes that companies have to subscribe to. And it is not just the payments industry; it is every company in the country that has to subscribe to these 47 different regimes. They all appoint different time, place, and manner for the notification. They all have different triggers for what kind of notification has to take place.

Some of them are even contradictory. There is one State that actually requires the breach notification to include detailed information about the breach itself. There is another State that makes it illegal to include any information about the breach itself. So, in some cases, they are contradictory.

If we had a uniform national standard, it would allow everyone in the ecosystem to work together toward the same goal, which is to provide that reasonable notice that needs to be provided as quickly as possible.

Chairman HENSARLING. In my remaining time, Governor Pawlenty, back to you. Our colleagues on the Energy and Commerce Committee have reported a piece of legislation with regard to a national breach notification law that only impacts retailers. Should this committee not act, from your vantage point, what does the world look like if that Energy and Commerce bill becomes law?

Mr. PAWLENTY. Mr. Chairman, I know time is short. Don't let the perfect get in the way of the good. We would like to have these standards apply across-the-board, otherwise, their effect is diluted.

We can be really good, but if our partner in payments has a flawed, outdated, weak system at a point of sale or in a back room at, say, fill-in-the-blank retailer or a different sector, the whole chain of events gets compromised.

So it is only as good as the whole chain. And if you just do one piece, you are missing a very important part or opportunity to up the game of the whole system. It is an ecosystem. It has to be addressed holistically, or the whole system is compromised.

Chairman HENSARLING. My time has expired.

The Chair now recognizes the ranking member for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman.

First, I would like to thank Mr. Carney and Mr. Neugebauer for the work that they have done on this legislation.

I believe that both sides of the aisle are concerned about getting a strong piece of legislation that will protect our consumers. This is a bipartisan issue, and we should not spend a lot of time fighting about some aspects of this initiative, but, rather, we should work out whatever the differences may be.

From what I understand, there are those who believe that the Federal law should be a floor rather than a ceiling. And there are those who believe that, where you have States who have stronger laws, we should not preempt those States.

As I understand it, despite the fact that we have varying laws in our States now, they all have similarities. And so, rather than thinking about this as States with such different laws that would somehow cause great complications, let's think about this in terms of the fact that we want our State attorneys general to be involved.

We want them to be involved in enforcement. I think that is very important.

So let us take a look at what I think is the biggest obstacle to us getting the best legislation and deal with the preemption question and think about States like California.

Ms. Moy, can you tell us, for example, in my State of California, what are we doing with the cybersecurity? And is that stronger than what is being proposed here now?

Ms. MOY. Sure. Yes. Thank you.

That is a good question and a good place to start because California passed the first breach notification law years ago and has really been a leader in this area. So thank you for your work on that.

For one thing, California recently passed a law to include log-in and password for account authenticators, so not just for financial accounts but for other types of accounts as well. For example, my email account, if my log-in and my password were breached, I would get a notification, which I certainly would want to, because there is a lot of information in there that, while it may not lead to financial harm, could lead, certainly, to emotional harm if that information were breached and if it were misused.

California also has a reasonable security standard, much like the Federal standard right now, but California does enforce that standard and has had a number of cases over the past few years and, along with that, has some very rich guidance for businesses attempting to comply with the reasonable security standard.

So one thing that I think California is also very strong on is the type of guidance that the State AG's office provides to the consumers and the way that the State AG's office interacts with consumers and businesses to provide that important guidance.

Ms. WATERS. Thank you very much.

I am sure that none of us would want to interfere with States' abilities to have the strongest possible laws for cybersecurity.

And so, Ms. Moy, don't you think that perhaps the Federal law should be a floor and that we should certainly allow States that have tougher laws to be able to enforce those laws? And that would require the attorneys general to be involved. Do you think that is the best way to approach this?

Ms. MOY. I do think from the consumers' perspective, that would provide the strongest protection.

And you had mentioned previously that there is a discernible pattern among the various States' laws. I think that is the case. When you look at the various breach notification laws of the States, most of them cover a core of common information and have very similar requirements in terms of what ought to be provided in the notification, when the State AG and the consumer reporting agencies ought to be notified.

And then, in addition to that, some States have added on to that. And so that is where, for example, you see States like Texas and Wyoming and just this year Hawaii and Montana have added medical information to the class of protected information in order to extend protection to categories where they see a developing threat that must be addressed.

Ms. WATERS. So we certainly would not want Texas to be preempted, with the good law that they have, particularly as it relates to medical information, would we, Ms. Moy?

Ms. MOY. I do think that it is important not to preempt the protection for pieces of information like medical information in, including other States, the very State of the chairman, Texas.

Ms. WATERS. Thank you very much.

And I yield back.

Chairman HENSARLING. The Chair understood the subtle point. The Chair now recognizes another gentleman from Texas, the chairman of our Financial Institutions Subcommittee, Mr. Neugebauer, for 5 minutes.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

I would note that if you let the Federal standard be the floor and all the States then have an opportunity to start one-upping each other, then basically we are right back where we are now, and it defeats the purpose of having a Federal standard.

Mr. Dodge, in reading your testimony last night on our proposed data security legislation, there is actually a lot that I think you and I agree on. I am hoping that maybe today we can discuss some of the provisions where we maybe have a little bit of a difference of opinion, in hopes that we could have a better understanding of where everybody is on this issue.

On page 7 of your testimony, you state, "Retailers support a carefully calibrated, reasonable data security standard."

Under H.R. 2205, Mr. Carney and I laid out a data security standard that is process-specific and based on certain key elements of data security programs that have worked well under Gramm-Leach-Bliley. To ensure the smaller retailers are not unduly burdened, we calibrate the standard to match the size, scope, and type of information that those entities hold. Where there are some process requirements that don't apply to you, you don't have to necessarily implement them.

So the question is, can you identify the specific processes we have laid out that aren't carefully calibrated and reasonable, in your estimation?

Mr. DODGE. Thank you for the question.

And I think, first, it is important that we are having this debate about proper national data security standards to help businesses address this growing and sophisticated threat.

It is the perspective of retailers that the Gramm-Leach-Bliley Act, which is the baseline for the legislation you introduced, especially the data security standards within it, were expressly written for the financial services community. The industries are very different. Anybody who has ever filled out a mortgage understands that the information that a bank holds is very different from that of a retailer.

If we were to pursue legislation that replicated the—or shoehorned the Gramm-Leach-Bliley Act to apply to the rest of the business community, we would be applying this law to industries beyond the retail industry, of course, well beyond us, into high-tech, Internet, app makers big and small.

And so we think that the history of enforcement through the Federal Trade Commission provides a good standard that is very

clear and strong for businesses to adapt to, to meet today's challenges, and it evolves for the future.

We don't think that you can regulate your way to security, that we need to employ layers of security. We need to start with the baseline that we believe is a strong standard and embolden the Federal Trade Commission to enforce these standards and then look at other ways for us to work together, including strengthening the payments system by advancing the security that is in that system today.

Mr. NEUGEBAUER. Now, you mentioned, I think, 50 FTC enforcement actions since 2001. That would be 3.1 a year. And so, if you believe that the FTC is your enforcement agency, do you support giving the FTC rulemaking authority to make a uniform standard?

Mr. DODGE. The FTC has enforced these cases under the Unfair and Deceptive Practices Act or Section 5 of the FTC Act. We think that giving them the express authority from Congress is the right way to go about it, and it would preserve that flexibility that they needed in order to adapt to the threats as they changed over time.

Mr. NEUGEBAUER. Yes. The question is, would you support them then promulgating standards that make sure that the playing field is level and that you are doing the things that are specifically necessary in your industry to have a uniform standard?

Mr. DODGE. We wouldn't support rulemaking, because we think that is the purpose of passing a law. We think Congress has the privilege of defining the law and then leave it to the agency to adapt it over time. They have the flexibility under current law—

Mr. NEUGEBAUER. Isn't that what we are trying to do, then? Congress is trying to pass a uniform standard—

Mr. DODGE. Exactly. And we believe that providing the FTC the authority to enforce data security laws based on the case law today, the common law based on the 50 cases, would provide businesses not only with the clarity that they need on what the expectations are of government but the flexibility for the enforcement agency—in this case, the FTC—to evolve over time to meet new threats.

Mr. NEUGEBAUER. So do your members take steps to protect consumers' data?

Mr. DODGE. Absolutely. There is no more important relationship in the retail business than that which they build and maintain with their customers. And obviously a breach, a data breach, would be a breach of trust with those consumers. They work extremely hard to prevent data breaches.

Mr. NEUGEBAUER. So, if they are already doing it, what is the objection, then, to just codifying that those are standards and they are reasonable and they should be applied across the industry?

Mr. DODGE. You are speaking specifically about a law that was written for the financial services community.

Mr. NEUGEBAUER. I am talking about the law written for—I am talking about my bill.

Mr. DODGE. Right. So , which you would be expanding under your legislation, expanding Gramm-Leach-Bliley to the rest of the business community. What we are saying is that we should stick within the current regulatory structure that has the Federal Trade Commission as the regulator for most industries, and Gramm-Leach-Bliley can remain for the financial services community.

Mr. NEUGEBAUER. Yes. We took principles from that, but this isn't a Gramm-Leach-Bliley rewrite. This is a uniform national Federal standard.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Delaware, Mr. Carney.

Mr. CARNEY. Thank you, Mr. Chairman, and thank you to the panelists for coming today.

I would like to talk a little bit about this preemption issue because I know it is a concern for many of the members, and we have worked hard to try to address it.

I said in my opening comments that the preemption provision in our bill should not have unintended consequences outside the issues covered in the bill. So we don't believe that it affects the medical debt issue which was raised a moment ago with respect to California. We would certainly be willing to make that plain.

Ms. Moy, I thought I heard you say that 50 different standards is not the answer. Is that what you said, or did I mishear your comments?

Ms. MOY. What I have said is that I think that the best for consumers would be to create a floor not a ceiling so that States can continue to—

Mr. CARNEY. So set a national standard and then allow States to—

Ms. MOY. Allow States to protect additional categories of information. For example—

Mr. CARNEY. Right. So my understanding is that 13 States currently have data breach notification and standards like this, and that our legislation, our Federal legislation, would be better than all of all of them, except maybe one, which is Massachusetts, and I have been talking to some of my colleagues from Massachusetts.

Would you agree with that?

Ms. MOY. I think that Oregon also has a pretty good standard, and I also think that there are elements of other State laws that you might not consider specific data security lawsuits, but they do have elements—

Mr. CARNEY. So a pretty high standard.

Ms. MOY. It is a pretty high standard, yes.

Mr. CARNEY. So that is the starting point for us.

How about the—there has been some discussion about the standard in Energy and Commerce. Would you say that is a high standard or a higher standard than what our bill would propose or—

Ms. MOY. That standard is a reasonableness standard that looks more like what the Federal Trade Commission is currently doing. And so I think the difference here is not only might be there be a difference in what the language says in that bill, I think also, we would be looking to the common law of the Federal Trade Commission and others to flesh out what the specific requirements are. But it is also really important as we are thinking about how strong the security standard is to think about who has the enforcement power and who is actually going to be guiding the parties there because if the Federal agencies are solely responsible for it, then even a very strong standard might not provide a strong protection as a general reasonableness standard that allows State AGs to continue

to work on a piecemeal basis with entities that are trying to comply.

Mr. CARNEY. Okay. So you think that the standard in our bill is a pretty good, pretty high standard in terms of a Federal standard, but you believe that the States ought to have the flexibility to go beyond that, notwithstanding some of the issues that might create in terms of having different standards.

How about this enforcement question? Have you looked at our bill in terms of the enforcement provisions in the bill, and how would you suggest that they be improved, from your point of view?

Ms. MOY. I have looked at it, but unfortunately, I am not prepared to provide a detailed response on the enforcement provision. So I would be happy to respond in writing if you would prefer that, but I do think that the key issue with respect to enforcement is that I believe your bill would only facilitate enforcement by Federal agencies, and, as I said, I really think—

Mr. CARNEY. You have said a number of times—I think what I heard you say is that allowing the State AGs some kind of role there would be an improvement, again, not having looked at the details there. Not to put words in your mouth.

Ms. MOY. Yes. I believe that a very critical element here is that we must have enforcement authority.

Mr. CARNEY. I explore these issues just because, as I said in my opening statement, Mr. Neugebauer and I are willing to try to improve the bill so that we can get a greater consensus around—we believe, I think as you said, that a national standard is important to have, and 50 different standards is not the way to go. It has to be a high bar and one that is enforceable.

Would any of the other panelists like to comment on the conversation that we have just had about preemption, about the standard and the enforceability of that standard?

Mr. OXMAN. If I could, Congressman Carney, I think the bill on a bipartisan basis really takes on this issue in the right way, and that is to recognize that the act of legislating to unify 47 disparate State regimes with a Federal regime that is not preemptive would merely be adding a 48th regime and wouldn't serve the purposes that the legislation seeks to undertake, which is to protect consumers' financial information. And, from ETA's perspective, the bill takes the right approach to ensure that the Federal regime is operative and is not interfered with.

Mr. CARNEY. And everybody agrees that we need a higher standard and kind of one standard across the country?

Mr. DODGE. We fully agree that there should be a national standard. We think that the States deserve a tremendous amount of credit for having acted in a place where the Federal Government has not yet. And that is why we believe that, as a broad concept, preemption—a strong law should offer State preemption and, as a broad concept, State AGs should have the ability to play a role in the enforcement of it.

Mr. CARNEY. I see I am out of time.

Thank you, Mr. Chairman.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from New Jersey, Mr. Garrett, chairman of our Capital Markets Subcommittee.

Mr. GARRETT. Thank you, Mr. Chairman.

Thank you for holding this hearing on an issue that really hits home for a lot of folks.

Let me just start—I also have a couple of questions—with the basics, if I can.

And, Governor, I will throw it to you.

When there is a breach or if someone does steal your card and they go to a retailer and buy a TV, who actually is responsible for that? Does Target have to pay the bill for that? Is it the bank or is it the Visa or MasterCard or Discover that is paying for that?

Mr. PAWLENTY. Congressman Garrett, the answer is a little complicated, but the oversimplified version is that—

Mr. GARRETT. That is what I am looking for, the oversimplified version.

Mr. PAWLENTY. The consumer is made whole, and the issuing bank is the one who makes them whole.

However, there is a secondary process managed and run by contract between the payment networks and various players in the payment system that gets resolved through a, shall we say, contractual process between Visa and MasterCard retailers, merchant acquirers, the issuer—people take issue with how that all works from time to time, but that is how it gets sorted out after the fact.

Mr. GARRETT. Oh. Okay. Does anybody else want to give an over—

Mr. DODGE. I would just add to that, yes, it is obviously—the merchant ultimately pays for fraud in the wake of a data breach, should the data breach have occurred at a retailer. They also pay a variety of fees. There are three real fees that they pay in total. The first one is on every transaction ever processed. It is an interchange fee. A component of it is a prepayment of fraud or prepayment of the data breach should one ever occur. And then post-breach there is a fee associated with reissuing the cards and—

Mr. GARRETT. Right. So that is where the banks actually end up having to pay the 15 bucks or whatever it is to actually pay to send me a new card every so often.

Mr. DODGE. But the merchant reimburses for those fees based on a—

Mr. GARRETT. Really? Because I hear different stories on that.

Mr. DODGE. Yes. I have included a schedule of that repayment in my written testimony.

Mr. GARRETT. I will look it up.

So, I just got one of these cards that have the little chip on it. And, also, just to be clear on this, putting this chip on the card may help to some degree as far as the lost card or the stolen card and the data breach as far as going to the retailer, but as someone else on the panel said, and I know it was in the testimony, this chip does absolutely nothing with regard to when they steal that information and they use it online. Is that correct?

Mr. DODGE. I think it is important to note, the chip—the technology that is available in the United States today, predominantly the magnetic stripe, is 1960's-era technology. Europe introduced something called chip and PIN technology more than a decade ago.

Mr. GARRETT. Right. And, in Europe, my understanding is that you saw an uptick of the data breaches not on—at the store anymore or the retailer anymore but now online. Is that correct?

Mr. DODGE. That is true. In fact, fraud moved in two directions when chip and PIN went into place in Europe. It moved online, and it moved to the United States because suddenly the United States had the weakest security in the world. It still does today.

When chip-only goes into effect later this year, the United States will still have the weakest card technology in the world.

Mr. GARRETT. Right. And somebody said—and maybe down here. You said that all—we can't solve all this stuff, and putting—so the bottom line is, doing the chip is not going to solve it entirely, but also to the point of what seems to be a lot of discussion in the bill as well as far as the disclosure information that—as Ms. Moy is talking about a lot and others as well—that doesn't do anything to—actually none of this—that doesn't do anything to do as far as preventing the fraud in the first place. That just tells me as a consumer: You were robbed, and now this is who is going to pay for it.

Mr. OXMAN. Yes. Congressman, if I could answer your specific question about the chip, you are absolutely right. The chip in the card prevents the card from being counterfeited.

Mr. GARRETT. Yes.

Mr. OXMAN. And that is today the number one source of card fraud in the United States. It is about two-thirds of card fraud at retail, but it does not address the online issue.

The online fraud issue is addressed by those other layers—

Mr. GARRETT. And really quick on this, because my time is running out a little faster than I want it to, the data that is on the card when I use this chip and I put it through has my number right on it. I hope nobody can see this. Does the retailer keep that information?

Mr. DODGE. The retailer transacts that information—

Mr. GARRETT. Yes. So they have that information. So if somebody now breaches in—

Mr. DODGE. But retailers are instituting—many have and all are moving towards it to make sure that information—

Mr. GARRETT. So it is still a place that—it is still a target for, not to use that company, but it is still a target for the hacker to go into the—or any of them. Not—medical or whatever. The hospital keeps that information too, I guess as a data source where they will go, try to breach it, and they won't be going to the retailer to use it, but they will be doing it online. So it is still a target and maybe even a larger target. Is that true now with the chip? Gosh, my time is going quickly. Is it a larger target because of that well?

Mr. ORFEI. I think it is important that we recognize the chip technology is really designed to button down the point of sale to defend against counterfeit, lost, and stolen. It is but one critical layer of security. There are other technologies that have been referenced in testimony here today, such as point-to-point encryption and tokenization, that will protect that data from the cyber breach you are referencing, Congressman.

Mr. GARRETT. Okay.

Ms. MOY. If I may just add a short comment in response to the point about notification and—

Mr. GARRETT. Fine with me.

Chairman HENSARLING. Short.

Ms. MOY. Thank you. Thank you so much.

Yes, I just wanted to say I think that notification does actually provide an important incentive for companies to keep information more secure. I can't remember actually whose written testimony it was, but someone's written testimony pointed out that companies do suffer reputational harm as a result of reporting breaches. And I also think it is important because that provides information to consumers who are considering where to vote with their wallet, so to speak, as they are determining which service to go with.

Mr. GARRETT. I get that. Thanks.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentlelady from New York, the ranking member of our Capital Markets Subcommittee, Mrs. Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman, and Ranking Member Waters, for putting this hearing together. It is an incredibly important issue because it affects everyone: consumers; government; retailers; and financial institutions.

And I also want to commend Mr. Carney and Mr. Neugebauer for putting forward a bill that would create a national data security standard for all businesses that handle sensitive financial information for consumers. And this bill would significantly strengthen the data security procedures for businesses but in a way that is flexible and can evolve as cyber threats change and evolve.

I am still concerned about the scope of the state of preemption in the bill, and I want to keep working on the preemption and enforcement provisions, but I have signed on to this bill as a cosponsor because I think it is a serious good-faith effort to tackle what is a critically important issue to our economy.

And, again, I would like to commend Mr. Neugebauer and Mr. Carney for their hard work and leadership on this issue, and I look forward to working with them, particularly in the enforcement provisions in it.

My first question is to Governor Pawlenty. I would like to ask you about the data security standards that Gramm-Leach-Bliley put in place for the financial institutions. You mentioned they had worked well in the financial institutions, but I also want to know, have they proven to be overly burdensome for smaller banks and credit unions?

Mr. PAWLENTY. Congresswoman Maloney, no. The standards have been flexible, and I think Congressman Neugebauer and Congressman Carney have done a good job in doing the same thing in their bill, which is to say: Look, we are going to have standards, but we are going to allow them to be scaled to the size and complexity of the enterprise in question. I think that is a good model.

Mrs. MALONEY. In other words, they have worked well and not been too burdensome for smaller financial institutions, and they won't be too burdensome for smaller retailers.

And I would also like to know your feelings about having a minimum or a floor standard. I know that California and Oregon have

a standard that is higher. I think it is important—you have to have a floor. Do you think it should be a floor, or do you think it should be a ceiling, and why?

Mr. PAWLENTY. Congresswoman, again, another great question, and if—right now we have nothing—

Mrs. MALONEY. Right.

Mr. PAWLENTY. —in many sectors. So something is better than nothing.

Mrs. MALONEY. Absolutely.

Mr. PAWLENTY. And so the floor would be progress, but a ceiling if it is set high. I would just encourage you—in Minnesota, when I was Governor, we passed what we thought were Nation-leading data protection standards and notification standards. You wouldn't want a bill that undercuts the 13 or so States that have done this. If you are going to set it, set it high. Set it aspirationally, and I think that would be the best place to be, and it would serve the country best. And think about the way that people place data centers, where they store data, how they store data. The fact that there is going to be wide variance between States doesn't sync with how we know cyber commerce gets done.

Mrs. MALONEY. But as a Governor, you know how valuable the creativity of the State system is to come out with solutions that—and are adopted in this area. It seems to evolve every day with new technologies, new ways to threaten consumers, and really the security of our information.

I would like to ask Stephen Orfei, given your organization's experience in establishing data security protocols and procedures, what would you say are the most important aspects of a company's data security plan? In other words, what is the most important thing that a company could do to protect their customers, to protect their company against data breaches?

Mr. ORFEI. Thank you, Congresswoman, for that question. I think what is most important is that the PCI standard is, in our view, the best defense against cybercriminal attacks. It really becomes a question of vigilance and being methodical and disciplined in your approach and looking at and paying special attention to the fundamentals. Doing the blocking and tackling. Looking at the physical and logical security. It is day in and day out. It needs to be 24/7. It needs to be built into the DNA of an organization from the CEO right down to the working level.

Mrs. MALONEY. Okay. Thank you.

And you mentioned in your testimony, Mr. Oxman, that you thought that sharing information was so important, and can you just expand on that, on what we need to do additionally in expanding information in this area?

Mr. OXMAN. Thank you, Congresswoman Maloney. The issue is companies are barred from sharing cyber threat information with each other and, in some cases, even with the government. The House fortunately passed a measure that we support that will eliminate those impediments to that kind of important information sharing. We support that legislation. We hope the Senate will move forward on it. And we need to make sure that companies can, without liability, share information with each other and the government to prevent future threats.

Mrs. MALONEY. Okay. Great. Thank you. My time has expired. Thank you.

Chairman HENSARLING. The Chair now recognizes the gentleman from Missouri, Mr. Luetkemeyer, chairman of our Housing and Insurance Subcommittee.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

I am kind of curious—I want to approach this from a little bit different angle this morning from the standpoint of, when we have a data breach, whose fault is it? If there is somebody at all, there is going to be some liability. It would seem to me—and my experience has been from the—of institutions I have been aware of, and I appreciate the Governor’s description a minute ago of who winds up paying the bill on this, but generally the banks wind up—or the financial institution who issues the cards originally are the ones that wind up footing most of the bill.

And it would seem to me to be that at some point, as a regulator, I would think that you would go into a financial institution and see a number of retailers, a Target line of credit, for instance, or any other local line of credit—in our area, we had a supermarket that issued debit cards. The information was accessed, and suddenly everybody in the whole area—whole region, actually, their information was breached, and as a result, there was a tremendous cost to the financial institutions. And it would seem to me that as a regulator, you would look at this as a liability exposure for the bank from the standpoint of what you are going to have to incur by all of these retailers not having adequate protections.

From Mr. Dodge’s perspective, it looks like—I would think that the regulators would ask the financial institutions to force the retail folks to have a policy in place, an insurance policy in place that would protect them against a data breach so that the banks would not be the fallback position for a data breach.

Governor, would you like to comment on that thought process? Am I off on that?

Mr. PAWLENTY. I think you have connected the dots exactly correctly, Congressman, and I think on your last point about cyber insurance, that is an evolving area. There are some who think their traditional insurance covers it. There are some disputes around that. There is some uncertainty about how you underwrite it when you can’t get your arms around the magnitude of it and what it looks like in the future. So that is an evolving and developing space, and one that is—

Mr. LUETKEMEYER. How do the standards fit into that situation?

Mr. PAWLENTY. The standards fit into that because I think if you set standards, like the financial services sector has, on other sectors and we get more resilient better systems as a result of that, you decrease risk. You de-risk the system. That is good for financial institutions. It is good for the payment system. And, frankly, it is good for everybody involved.

I will say to the chairman’s point on Energy and Commerce’s bill, that is a bill that says, “Have reasonable standards.” We are going to get a standard one way or the other in this country because everybody is suing everybody. And, over time, the courts are going to develop a standard, and it is going to say, “Be reasonable.” And that is a 10-year pathway. It is too slow, and it is too vague. Or

you are going to have a bunch of States doing a hodgepodge of standards, some of which will be great, and some of which will be not so great. So Congress can play a really important role here bringing this debate forward more quickly and at a more—a level of rigor in the standard, and it will help.

Mr. LUETKEMEYER. Mr. Dodge, would you like to comment on my question?

Mr. DODGE. Yes. First, the suggestion that banks are not reimbursed in the wake of a data breach is simply not true. As we talked about earlier, there are three major ways in which they pay, and there are certainly more than just those three. But the first is in the fees that they pay on every transaction. Then, after a breach, through the contracts that they sign with the card networks, there is a formula for reimbursement which—

Mr. LUETKEMEYER. They still suffer a loss, Mr. Dodge. From a business, I can tell you—

Mr. DODGE. But the issuing bank—the issue is—if the banks have an issue with that, it is with their facilitator, which in this case is Visa and MasterCard. Retailers sign those contracts, and if there is a suggestion that there has been a violation of those contracts, then there is certainly the legal avenue for resolving that.

Mr. LUETKEMEYER. Okay. My question, though, is with regards to the exposure, liability exposure, that a bank would have with regards to this situation. You have lots of retailers. And this seems to be almost an epidemic. Every week you have another entity that has been breached. If that is the case, pretty soon those institutions are going to have a tremendous liability sitting there. And if you have lots—if you do a lot of commercial lending to retailers, I see that as a problem that is going to have to be fixed. And I would assume that you would be supportive of the idea of having the retailers purchase a liability policy of some sort that would protect them as well as the institution against a breach.

Mr. DODGE. As Governor Pawlenty said, the cybersecurity insurance market is a new market, but many retailers are buying that kind of insurance. There is no question about that. But the level of standard—the suggestion that there are no standards on retailers is belied by the fact that there were 50 cases, some of which were retailers, but many were not, where strong enforcement was brought down by the Federal Trade Commission, enforcement of that includes not only substantial fines, but the prospects of consent decrees that allow the Federal Trade Commission to take up residence in the business for 20 years. So there are very, very strong standards that retailers are bound by today.

Mr. LUETKEMEYER. I just have a few seconds left. Just one comment: Mr. Orfei, I am disappointed that you gave everybody my password to my computers.

But with that, I yield back. Thank you, sir.

Chairman HENSARLING. The gentleman yields back, and he better put a fraud alert on all of his credit cards.

The Chair now recognizes the gentleman from California, Mr. Sherman.

Mr. SHERMAN. Governor Pawlenty, I do weird things that cause my credit card company to get very concerned, like I buy gasoline in Los Angeles, and a day later, I buy gasoline in Washington. So,

of course, their computers flip out. And you would think what they would do is send me an email. But they don't. They either call me, usually at the worst possible time, or if they are too lazy to do that, they freeze the account and force me to call them.

Is this entirely because they are not handling it right, or is there something in our statutes that we could do to facilitate or prod credit card companies to check with their cardholders by email rather than by telephone?

Mr. PAWLENTY. Congressman, great question. I have had some interesting experience with cards myself personally. So—

Mr. SHERMAN. You engage in similar unusual activity?

Mr. PAWLENTY. I am not admitting to unusual activity, sir, but anyhow, as to—

Mr. SHERMAN. Another guy—we have another guy going to Iowa.

Mr. PAWLENTY. I think the concern that you raise is a good one, but it is being addressed in realtime by technology. The controls that you can now set on many cards—and it is advancing by the day and the month—are getting really good. So, for example, on one card that I have, I can get a text or email alert if it goes over a certain amount, any transaction. I can get a text or email alert if it goes over a certain number of transactions per month. I can get a text or email alert if it goes over a certain amount. And soon, I think, I am going to be able to get an alert if—

Mr. SHERMAN. I am not looking for more alerts. I am simply looking for them to contact me by email rather than by phone, rather than by freezing my account without telling me about it.

Mr. PAWLENTY. The short answer is, I think if you can't, many cards already do or will soon offer you the chance to be in the driver's seat as to exactly how you want to get that message.

Mr. SHERMAN. I am sure your members are aware of email—we are here talking about how to upgrade to technology, and I am hoping that email is—

Mr. PAWLENTY. If you can't, I can recommend a card that—we will get it to you.

Mr. SHERMAN. Yes, but not with the United Airlines miles.

Basic economic theory is that you apply liability against the entity that should be investing in safety measures so that you get that entity to spend the appropriate amount of money on safety measures.

Retailers ought to be spending more on safety to protect consumers and to protect the entire business system from the extraordinary costs that happen every time somebody hacks into one of these accounts. But retailers face no liability except the reputational liability, which Ms. Moy referenced.

But then we have these lesser known data breaches where the media doesn't know or barely reports to the general public some of the data breaches.

Is it problematic that consumers at some stores may have their data hacked, but they never hear about it? And does this mean that the merchant that has mishandled the data faces no liability and no reputational risk?

Ms. Moy, in order to have that reputational risk, do we have to do more to make sure that every data breach is known by the public?

Ms. MOY. Yes, I think we do. And I think that there are a couple of ways to do that. And one is to make sure, as I mentioned multiple times, that the bill is written in such a way that it covers classes of information that entities may hold that consumers consider personal but they would want to be notified about but currently might not be notified about. So, for example, email address and password. That is one that a lot of retailers hold. It is one that could be breached. If my email address and my password are breached, I would certainly like to know about it.

And another thing that could be done is, again—sorry to be a broken record—but providing State AGs with the authority to enforce is really important because they will help work to make sure that these breaches are notified. And, in particular, many States have a threshold for notification of State AGs and for consumer reporting agencies that is much lower than what we have in a lot of Federal legislations. And in a lot of the Federal bills that we have seen proposed, the threshold would be 10,000 affected consumers. Many States have a threshold of 1,000, for example.

I believe that just a couple of months ago, the Massachusetts State AG's office appeared at another hearing on breach notification and data security and they said that the average breach—the size of the average breach was about 74 consumers. So it is really important that we have State AGs working to ensure that consumers are notified.

Mr. DODGE. Congressman, if I could just jump in on that?

Mr. SHERMAN. Yes, and I will add another question and let you jump in on both.

We are proposing Federal legislation. Is the work of the State AGs and the States enough to prod retailers to spend enough on safety?

Mr. DODGE. So, to your question about liability, retailers face considerable liability. Obviously, there is reputational harm. You cited that. But under the enforcement available through the FTC's current authority and what we have endorsed for stronger authority and at the State level, there is enforcement liability and the prospects of consent decrees that could take—allow the FTC to take up residence in a business for 20 years.

Mr. SHERMAN. I will see if the Governor can just chime in.

Do the retailers face enough reputational and financial liability to spend enough on safety, or do we need to do more?

Mr. PAWLENTY. Congressman, I would respond with a rhetorical question. How is the current system working? Not so good.

Mr. DODGE. The Verizon report, which is the gold standard for reporting on data breaches, says there were 2,100 breaches last year: 277 were financial institutions; 166 were merchants. There were 1,000 times more merchants. So the standards that are applied to the financial industry are not perfect.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Michigan, Mr. Huizenga, chairman of our Monetary Policy and Trade Subcommittee.

Mr. HUIZENGA. Thank you, Mr. Chairman.

And I appreciate the opportunity to spend a little time with you all.

Mr. Orfei, while we are on the breaches, I would be remiss not to say that Mr. Garrett's credit card has now purchased at least three things online and is available widely on a Russian Web site.

But, in all seriousness, that is the concern all of us have. Right? When we are calling in somewhere or buying something online in the very transient kind of economy that we have, I think we all have a legitimate and serious concern.

But I am curious, Mr. Orfei, from your perspective, have you evaluated how many breached companies are in compliance with your PCI standards at the time of their breach? Or have they had those standards, and then it has caused them to take action? Or did they have them already, and they still were breached?

Mr. ORFEI. What I would reference is the Verizon report, which is an objective third party that looks at the data for breaches for the past 10 years. And the findings—there are two significant data points that I would give you, Congressman. One is that 99.9 percent of the breaches that have occurred were preventable and covered by the PCI standard.

The second point is that I think that the PCI standard has done a very effective job, and there hasn't been one single compromise where the merchant or the entity was found in compliance.

Mr. HUIZENGA. Okay. I am a former State legislator as well, and, Governor, it is good to see you again.

And I, like you, had those situations where we were sitting in the State capitals saying, "What in the world is Washington trying to do to us now?" Yet, at the same time, I understand when you have States doing various actions and not coordinating, and oftentimes that is somebody like the Council of State Governments and ALEC and other organizations like that are trying to get States to harmonize oftentimes.

But what I am struggling with on this—and, Ms. Moy, you had mentioned this earlier, as did my friend, Mr. Neugebauer—is how is setting a national floor but then allowing States to maintain a patchwork of other requirements different than what we have now? And I think maybe it was you, Mr. Oxman, who said we would go from 47 regimes to 48. So help me out, somebody, with what we do on this. I would love to hear from Governor Pawlenty.

Mr. PAWLENTY. Congressman, I would think about this—I am a big fan of the 10th Amendment. I am a big fan of States' rights. I am a big fan of laboratories of democracy for public policy at the State level. I believe in all of that profoundly. But I have come to think of this issue as a threat to the national security and critical infrastructure of the United States of America, not just in the payment space but in the ability to do most of what we do. And so I think it rises to the level of being worthy of being viewed in that light and setting the table nationally because it does threaten our ability to function. It presents, taken to any sort of reasonable extension, an existential threat to our economy and to our Nation's security. And I could walk you through the scenarios, and they don't take a lot of imagination. But I think if you view it in that light, it rationalizes an aggressive and muscular Federal involvement.

Mr. HUIZENGA. And that is where I struggle as well, and we can have a constitutional debate later, whether this is part of a commerce clause or how this is affected.

But, Ms. Moy, I don't know—quickly. Briefly.

Ms. MOY. Thank you. Thank you so much. Yes. So just to repeat again, I think most States certainly with breach notification, there is a common core of elements that we see across the various—across the 47 plus, I think, three territories, laws. And then there are some additional elements above that. But I do think that it is really important. For example, I believe in your own State, there is a harm trigger for the breach notification law that is broader than just applying to financial harm. It is really important that we take that into account, as Governor Pawlenty has said. If we are going to set a preemptive Federal standard, let's set it high. Let's not reduce protections like those in your own for consumers who are benefitting from that.

Mr. HUIZENGA. And I would agree. I think it would have to be high. And somebody help me out on what—as Mr. Sherman had said, he doesn't want more notifications. Now, I am a little confused as to how, if you have an email breach, are they supposed to notify you through email if that has been breached? But what of this “cry wolf” overnotification, is that a real concern?

Mr. DODGE. Congressman, we think that it is. We think it is important and on—I align myself with the most recent points made by the Governor. We agree entirely on this. We think it is important that consumers be able to get information quickly and information that they can take action on in order to protect themselves from financial harm.

A standard beyond the financial harm would subject customers to repeat notifications. And the worst case scenario is the customer would stop paying attention to those notifications and not take action to protect himself or herself in the wake of something that could put them at risk.

Ms. MOY. If I may just add a brief point about that, which is that I think in order to determine the answer to that, we should really look to the State AGs, who have a ton of contact with consumers who are suffering from breaches. And in the words of Illinois attorney general, State AG—I'm sorry—Illinois Attorney General Lisa Madigan, “Consumers may be fatigued over data breaches, but they are not asking to be less informed about them.”

Chairman HENSARLING. The time of the gentleman has expired. The Chair now recognizes the gentleman from Massachusetts, Mr. Capuano.

Mr. CAPUANO. Thank you, Mr. Chairman.

I can barely see you guys. They kind of moved everybody apart, but we will try to communicate.

Mr. Chairman, I would like to submit a letter from the Massachusetts Attorney General for the record.

Chairman HENSARLING. Without objection, it is so ordered.

Mr. CAPUANO. Thank you, Mr. Chairman.

Did anybody at this table think that 5 or 10 years from now the data security—the issues and the challenges you face will be the exact same that you face today? Does anybody believe that to be true?

Mr. OXMAN. Technology is changing so quickly, Congressman, I think it is highly unlikely that the issues will be exactly the same.

Ms. MOY. Yes. I think it is highly unlikely. I mention in my written testimony the example of several apps that now exist that allow you to photograph your physical keys to your house and your car—

Mr. CAPUANO. That is great. Well, thank you. I don't think so either, but then, again, I don't know much about technology. I struggle with a cell phone. And that is life.

But the one thing I do know is that something is going to be changing, and I guess I raise the issue because to advocate for a congressional solution with no ability to change a year, or 2, 3, or 4 years from now when the problems change except to come back to Congress, you are sitting here today because the Congress is last to the issue. States are first to the issue, like in most issues. The Federal Government is oftentimes the last one to the fight because we are the biggest; we are the most diverse; and that is the way it has always been. And yet you are advocating for a situation that we have one great—let's assume it is a fantastic law that has no ability to be upgraded through regulation, which is why we have regulatory bodies, because they can act quicker than us, except to come back to us and ask us to do this all over again, which in and of itself, to me, is the main problem here.

But the other issue I ask, do—I don't know where any of you live, but I am going to presume that since I think you are all part of associations and like that you must live in the general Washington area, at least have an apartment here. Do you think that the Federal Government, the EPA, should tell the State of Maryland that they have to have only Federal standards on their drinking water, that the State of Maryland would then be totally preempted from saying, "No, no, no, we like a little less arsenic in our drinking water than the Federal Government requires, and, therefore, we would like to do it?" Do you think that the State of Maryland should be told, "Sorry, you can't do that?"

Mr. OXMAN. Congressman, I spent 7 years in the great Commonwealth of Massachusetts. I had the pleasure of living there for a long time, and I think you raise a very important question, and that is, how can we bring uniformity to an issue that has nationwide implications, and indeed international implications when we are talking about cybercrime without interfering with the power of the Commonwealth of Massachusetts?

Mr. CAPUANO. Not just the power, the responsibility, as I look at it. I actually like the idea. I am very happy that we are talking about Federal standards. I have gotten in trouble on a regular basis because what the heck, I am a liberal Democrat. I am all for Federal regulation. My friends over they, they know it. I would regulate everything. Don't worry about it. But then again, I didn't know that some of my friends on the other side apparently want to join the Socialist Party. They are welcome to; Bernie Sanders has cards and you can sign up.

That is my problem. I don't have any problems. I love the idea of creating Federal standards and a Federal floor, but I like two other things: I like flexibility in that because, let's be honest, most Members of Congress are not technologically capable. I know some

guys here, but every one of us fumbles with our cell phones. I call my staff all the time. I kick the damn things. I drop them. This one was broken 7 times because I threw it. And I know none of you have done that because you are technologically capable. We need flexibility. We need the ability to move quickly because whatever the threat is today is going to change tomorrow. That is the only thing I know.

Mr. OXMAN. That is right. And, Congressman, I would submit that ETA, on behalf of the payments industry, supports the approach that Chairman Neugebauer and Mr. Carney have taken in this bill because it has the exact flexibility you are—

Mr. CAPUANO. That is critical.

Mr. OXMAN. It doesn't dictate any technical standards. And, in fact, it makes very clear that it is not up to the Federal Government to dictate how we protect data security, but it is a requirement of the Federal Government that security be implemented.

Mr. CAPUANO. And we also have to have somebody who knows what they are talking about, not necessarily the United States Congress, number one. And, number two, I really don't see why you would want to take away the ability of the States to be more flexible than anybody else. Holding to a minimum standard? Absolutely totally agree. And, again, we have the same issue on everything that we do. Every financial issue we deal with, we deal with this issue. How much of a Federal standard, including, we deal with insurance every day. Insurance is totally regulated at the State level, and every time we come close to even thinking about the Federal involvement, everybody gets all worked up because the States do it. And I strongly suggest the concept is right. The approach needs to be significantly changed on those two issues, to provide flexibility, number one, and to maintain the States' ability to deal with it as they see fit. Thank you.

Mr. NEUGEBAUER [presiding]. I thank the gentleman.

And now the gentleman from Wisconsin, Mr. Duffy, the chairman of our Oversight Subcommittee, is recognized for 5 minutes.

Mr. DUFFY. Thank you, Mr. Chairman, and it nice to see that we are making news today with Mr. Capuano endorsing Bernie over Hillary, my good friend. Also great visuals of you throwing your flip phone around the Capitol.

As Mr. Huizenga said, he was a State legislator. I was not, Governor, but I was a former hockey player like yourself.

Do you agree with Mr. Dodge that the banks don't pay any fees when there is a data breach? I haven't heard you respond to that claim.

Mr. PAWLENTY. Congressman Duffy, the banks—again, the system of how this all gets sorted out is complicated, but it is certainly true that the issuing banks pay in all sorts of ways if there is a breach, including the cost of reissuing the cards, subject to possible partial reimbursement in the future, as well as making the consumer whole through a complicated series of transactions. So—

Mr. DUFFY. Okay. And just to be clear, does the whole panel support Federal preemption? Does anyone disagree with that concept? I think I have heard everyone say they agree.

Ms. MOY. Only if it is a high standard that preserves protections for consumers.

Mr. OXMAN. We support it.

Mr. DUFFY. Okay. So, quickly, just so I understand, talking about when the card is present, what percentage of the fraud comes from a fraudster who steals data and reproduces cards and makes purchases as opposed to the guy who had his wallet lifted, and someone goes in and uses actually the cards—

Mr. PAWLENTY. The majority of it—excuse me, Congressman. The majority of it is people scraping cards and using counterfeit cards. And the people who do the lost and stolen, some of that happens, but that is the minority of the transactions, not counting the online stuff.

Mr. DUFFY. So when we talk of chip versus chip and PIN, if we just at least get to chip, we are going to address a vast majority of the fraud that is talking place right now when the card is present. Is that fair to say?

Mr. DODGE. I would say in a static world, it would have an effect. But we don't live in a static world. The reality is that there is a single line of defense between the fraudsters and their ability to commit fraud. In this case, it would be chip. And they will focus all of their energy on breaking that. We have seen examples where they have done it already, and we have simply argued that one of the baseline tactics of cyber hygiene is two factor authentication. We should require that at the point of sale as well.

Mr. DUFFY. But by you saying that, are we going to see more pocket thieves out there?

Mr. DODGE. No, no, no. I am saying that fraudsters will develop new and innovative ways to crack the chip and commit fraud.

Mr. DUFFY. Is that happening—

Mr. ORFEI. Congressman Duffy, if I may—

Mr. DUFFY. You may.

Mr. ORFEI. —the chip will defend against counterfeit, lost, and stolen at the point of sale. It will button down the point of sale at physical environment. Once that environment is secured, fraud will then move to the card-not-present environment. It is what we observed in the Asia-Pacific and European theaters who have had chip technology. Now, the chip technology is—you cannot clone it. So what we will see is, it will migrate.

Mr. DUFFY. So how far away are we from tokenization for online purchases?

Mr. ORFEI. Tokenization is a technology that has been around for 10 years. And now the acquiring community and technology vendors and the price points have come down. So point-to-point encryption coupled with tokenization coupled with EMV at the point of sale is how we get to devaluing the data so that it is useless.

Mr. DUFFY. So if the card-not-present online purchases, the technology is there but just not implemented yet to secure—

Mr. PAWLENTY. Apple Pay has a—what I call an early stage version of—I don't want to say primitive—but early stage version of tokenization, and it has had some other breach issues, but it is kind of the first—one of the first kind of tokenization platforms to come to market.

Mr. DUFFY. I just want to be clear. So, when we have a chip, does a retailer—are they able to maintain data about the card in

their database if you just have a chip card as opposed to a magnetic strip?

Mr. ORFEI. Again, Congressman, the chip is just going to work at the point of sale. How that merchant stores data—

Mr. DUFFY. But can they store—so what my question is—listen. We have heard about all the retailers who have had data breaches. If we migrate to the exclusive use of chips, does that mean that retailers are no longer keeping personal consumer data in their databases, which means—

Mr. ORFEI. No. No, sir.

Mr. DUFFY. —they are not at risk to have breaches any longer?

Mr. ORFEI. No. Again, it is just taking off the threat at the point of sale. So it is a critical layer, but it is not a silver bullet.

Mr. DUFFY. But on the back end, retailers still keep information—

Mr. ORFEI. On the back end, the information could be replaced, though, by tokenization, could be protected by point-to-point—

Mr. DUFFY. Do you have recommendations on how long retailers are recommended to keep financial information about consumers? How long should a retailer keep that information?

Mr. ORFEI. It is really not necessary to keep that information.

Mr. DUFFY. So—

Mr. DODGE. Congressman, if I could just jump in.

Mr. DUFFY. Sure.

Mr. DODGE. A couple of things. First, many retailers have instituted encryption for that information when it comes in so that if it ever was acquired, it would be in a format where it would be useless to a criminal. Further, they have no desire to keep information they don't need nor to keep information—

Mr. DUFFY. But do they need any information, is my question? Could retailers, after 30 days, wipe those databases clean so you don't have 6 months of consumer data or a year of consumer data; you might only have 15 days or 30 days of consumer data? Isn't that really one of the risks that we have with so much data being collected and stored, not just from the government, but from retailers?

Mr. DODGE. The information that retailers collect is designed to allow them to provide the concierge-type services that they want. Consumers generally want receipt-less returns. So there is an element of information that consumers have voluntarily said: We want to be able to—you have this information so that we can do these—

Mr. DUFFY. I don't know that I have ever been asked to volunteer to enter into one of the concierge services. I think they are just offered to me, and that information is kept on my card. And I do think there is a consumer protection issue here when we are not asked, it is just given to us, and you keep that information on—my time—

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Texas, Mr. Hinojosa.

Mr. HINOJOSA. Thank you, Chairman Hensarling and Ranking Member Waters, for holding this important hearing today.

And thank you to our panelists for your testimony.

Mr. Chairman, before asking my questions, I request unanimous consent that my opening statement be made a part of today's record.

Chairman HENSARLING. Without objection, it is so ordered.

Mr. HINOJOSA. My first question is to the Honorable Tim Pawlenty and Ms. Laura Moy.

How can a Federal data security standard that creates a floor provide for more consumer financial security while at the same time providing certainty to industries that would need to implement such a standard across all 50 States?

Mr. PAWLENTY. Congressman Hinojosa, thank you for your question.

For certain sectors, not including financial services and health care and a couple others, they don't have standards currently other than in the 13 States or so where they have them. So, by Congress creating a floor or a ceiling—but we hope a high standard—that is for the whole country, you will lift the game and the expectations and the legal responsibilities for those sectors in those places that don't have a standard currently. And, again, this has migrated to international proportions, and I think if the members of this committee knew that Russia or China or semi-state agents were about to compromise the payment system, the electrical grid, you wouldn't say: Yes, let's kick it to the States; let's let them handle it. I don't think you would do that. So whatever you do will be helpful, even if directionally, it will be better than what we have now for those sectors that don't have any standard in those States.

Mr. HINOJOSA. Ms. Moy?

Ms. MOY. I would say a couple of things. One is that consumers are protected right now by the Federal Trade Commission Section 5 authority, and the FTC is enforcing that. As we have heard, they have enforced over 50 cases since 2001. And consumers in 47 States and 3 jurisdictions are protected by breach notification laws. So there are protections existing for consumers. I think setting a floor and not a ceiling, as I have mentioned before, there is a clear pattern in terms of what is covered even by the disparate State laws. So, as a practical matter, most companies that have to comply with the laws of multiple States are just complying with the strongest standard and are mostly okay under the other States, including—in fact, many States have a provision that allows an entity to notify some consumers who have been affected by a breach under the standard of another State.

But I would add to that, if we are going to have a Federal preemptive standard, as I said before, it has to be a high one, and it has to provide flexibility to adapt to changing technology, not only in terms of what the security standard is but also in terms of what information is covered by the bill. That is a critical element that I think we might be missing here.

Mr. HINOJOSA. Thank you for your response.

My second question is addressed to Mr. Jason Oxman and Mr. Brian Dodge.

Given the ever-increasing sophistication and sheer number of cyber attacks on our financial institutions and markets, do you think a catastrophic attack, which can have severe repercussions on the financial system as a whole, is imminent, and what can the

Federal Government do to help prevent such an attack or prepare to respond to such an attack?

Mr. OXMAN. Thank you for the question, Congressman Hinojosa.

The possibility of such an attack is always on the minds of the payments companies that ETA represents, and preparation for those attacks is, of course, something that is always included in all the operational plans of all the companies that we represent. Our sincere hope is that something like that never happens, but we do recognize the important role that the payments infrastructure plays in empowering commerce in this country. And protecting our customers, be they merchants or consumers, is always at the top of our minds. So we are focused on that. We are prepared for it, and it is our sincere hope that nothing like that ever comes to—

Mr. HINOJOSA. Thank you.

Mr. Dodge?

Mr. DODGE. So, in terms of your question about what Congress can do, I think the focus on data security to avoid such a catastrophic event is incredibly important. We believe that the way that you get yourself to a stronger environment is layers of security. And Congress can help with that by, as the House did last month, passing information-sharing legislation, but also as we are talking about today, providing clear and strong guidance for businesses on how they should maintain their systems to ensure cybersecurity, and then providing the flexibility for businesses and for regulators to adapt to that threat over time. There is no doubt that the threat is increasing. The level of sophistication is growing extremely fast. And we need to be able to stay involved in it.

The last point is we need to look to where our greatest vulnerabilities are, and right now our greatest vulnerability from the merchant community is the cards that we accept at the point of sale. They are the weakest security technology enabled in the world today, and when we move to chip technology without the PIN like has been instituted in the rest of the industrialized world, we will still have the lowest level of security in the world, and fraud will continue to flow towards us.

Mr. HINOJOSA. Thank you.

My time has expired and I yield back, Mr. Chairman.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from South Carolina, Mr. Mulvaney.

Mr. MULVANEY. Thank you, Mr. Chairman.

And thank you to everybody on the panel for helping us try to do something we don't do enough here, which is just try and collect information, which is what I am going to try and do. I am not here to try and beat anybody up. I actually have an honest-to-goodness question. And I think it is directed to Mr. Pawlenty and Mr. Dodge, but I would welcome everybody to chime in on this. Okay?

Let's say that Mr. Capuano steals my credit card, which is possible because he is that kind of guy, even though he is not here yet, and he goes to my local gas station or his local gas station, slides it in there, happens to—maybe he knows my ZIP code and buys the gasoline with my stolen credit card. I catch it when my statement comes in the next week or maybe I get an email notification, which I think is a service my bank actually provides, which I enjoy very

much. I catch it. I call my bank and I say, "Someone stole my credit card. And they just used it to buy gas in Massachusetts." And they say, "Okay, Mr. Mulvaney, thank you very much. We will take it off your bill."

Who eats that loss? Is it the retailer? Is it the bank that issued my card? Is it Visa or is it somebody else? Who eats that loss for that gasoline bought with a stolen credit card?

Mr. DODGE. First, I would say if a PIN was required in that transaction, the fraud would have never occurred in the first place. You wouldn't have had that.

Second, there is a difference between data breach fraud repayment and traditional fraud repayment. And so there would be, based on the contracts that the retailer signed with the card networks, an evaluation of where was the weakest link in the system. So if it was a stolen card and it was reused, then it would probably—actually, I don't know the answer to that question as how it would go, but it is determined by—

Mr. MULVANEY. Whoa, whoa, whoa. Is that—

Mr. DODGE. But in many cases, in almost all cases, fraud—an element of that fraud is charged back to the retailers.

Mr. MULVANEY. Mr. Pawlenty?

Mr. PAWLENTY. Initially, somebody has to give the cash back where it is a debit transaction or the value to—

Mr. MULVANEY. Again, it was a credit transaction.

Mr. PAWLENTY. It is the issuing bank, and then they sort it out afterwards as to who pays what. But, in terms of who eats most of it initially, in our view, over the long term of the discussion, it is the banks.

Mr. MULVANEY. All right. Mr. Dodge, and here is why I asked the question, because I have my banker friends come in, and they say, "Look. We have to do something about this because we eat all of this loss." And just last week, I had some of my convenience store people come in and say, "Look, we have to do something about because this because we eat all of this loss." Are both of them eating a little bit of the loss? Is that what it comes down to? I see some people in the back row nodding their heads, which is usually a good sign.

Mr. DODGE. I included in my testimony a schedule of repayment that shows the fees of the structure of the contracts that obligates merchants to repay in the wake of a breach. Those are reissuance costs, the cost to reissue the cards, and then fraud, fraud that is associated with the breach. But every single day on every transaction that is processed, a merchant pays a fee. It is called an interchange fee. Sometimes it is called the swipe fee. And an element of that fee is a prepayment of fraud. It goes into the account. Whether fraud happens or not, they are prepaying it every single day. So how that is divided up by the banks, is a great question for them. But we know we pay it on every single transaction.

Mr. MULVANEY. Okay.

Mr. OXMAN. Congressman, if I could—

Mr. MULVANEY. Yes.

Mr. OXMAN. The hypothetical you asked actually has a pretty simple answer, and that is the card issuer is responsible for that fraud. The lost and stolen fraud you described is never the respon-

sibility of the merchant. Since your card was stolen out of your pocket, and you hadn't yet reported it stolen when that card was used and the transaction was authorized by the issuing bank at the gas station, the issuing bank has a responsibility for that. You don't and the merchant doesn't.

Mr. MULVANEY. Thank you, Mr. Oxman, because I think that leads me to the next question, which is, does the analysis change—I think I got it now for a stolen card out of my pocket. Mr. Capuano steals my credit card. I get it. And he would do that too. He is—what if the card is counterfeit? Is it any different? If someone gets it from Target, gets my information from Target, and they create a counterfeit card and then use it, is the outcome any different? Is the distribution of who bears the loss different? Mr. Oxman?

Mr. OXMAN. So, as it stands today, the analysis is exactly the same. In the case of a counterfeit card, the issuer would have responsibility for that and the merchant would not.

The migration to EMV chips that we have been talking so much about this morning actually changes that calculus, and the responsibility for the fraud, after October of this year, will actually fall on the party to the transaction, whether it is the merchant side or the issuing side, that has deployed the lesser form of security. Not to get too complicated, but if that card that you are talking about has been counterfeited and it was a chip card and the issuer has issued chip cards but the merchant hasn't installed the chip readers, then the merchant will have responsibility for that fraud. So that is a change to the current system, which is the issuer takes responsibility.

Mr. MULVANEY. And then, finally, if I can have the indulgence of the chairman for 15 more seconds, the third example of the fraud we have talked about today is the online fraud, which is there is no card present, we are online buying airplane tickets. Who bears the risk of loss on that one?

Mr. DODGE. Merchant, 100 percent; 100 percent the merchant is subject to the fraud cost.

Mr. MULVANEY. I thank the witnesses very much. I really appreciate the information.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Missouri, Mr. Clay, the ranking member of our Financial Institutions Subcommittee.

Mr. CLAY. Thank you, Mr. Chairman, and I wanted to note that I am so glad to be back in this refurbished hearing room.

Mr. Orfei, you note at the end of your testimony that not a single company has been found to be compliant at the time of their breach, but in many cases, firms that have been breached were at one point PCI-compliant.

How does your compliance framework lend itself, if at all, to ongoing monitoring of the PCI compliance, and what role does the PCI play in monitoring compliance?

Mr. ORFEI. Thank you for that question. Yes, 99.9 percent of the compromises were preventable and covered by the standard. And if you think about our standard, what we are advocating is a move away from compliance to a risk-based approach, and we are advocating vigilance and discipline and being methodical in close adher-

ence to the standard. Security is a 24/7 responsibility. It is not a matter of compliance. What we see happens is a company works diligently to bring its organization into compliance. They high-five each other on Thursday, and on Friday, the environment starts to deteriorate. So it is about being disciplined, methodical, and paying attention to the fundamentals, sir.

Mr. CLAY. Thank you for that response.

And, Mr. Oxman, although chip technology is fairly new to the United States, it has been around for decades and is ubiquitous in other parts of the world.

Given the rapid pace of technological development, are we not at the point where other types of security measures are more appropriate for use in connection with U.S. payment cards and payments in general?

Mr. OXMAN. Thank you for that question, Congressman Clay. You are absolutely right that the chip is a well-developed technology, and the good news is the payments industry recognizes, as you have heard this morning, that the chip addresses one type of fraud. That happens to be the most prevalent form of fraud here in the United States today, and that is counterfeit card fraud. So the chip implementation will address that type of fraud. But, as you noted, other types of security are important as well, which is why our industry is deploying a layered security technology approach, which includes the chip in cards, but also tokenization, which replaces account information with a one-time use mathematical cryptogram that can't be intercepted and reused. It also includes point-to-point encryption, which secures all entry points into the payment systems. So that layered approach with multiple different technologies, as you suggested, is in recognition of the fact that the chip card addresses one type of fraud, but we need to do much more because criminals are much more sophisticated.

Mr. CLAY. Thank you.

And for anyone on the panel, how prevalent is fraud in the case of online checking? Is that pretty secure? Can anyone respond to that?

Mr. DODGE. Online checking?

Mr. CLAY. Yes.

Mr. DODGE. Certainly, e-commerce is an environment where there are limited security options for merchants to employ right now. It is a frustration of merchants. The fact that e-commerce is such a big part of the economy and there is no strong means of security is a considerable frustration.

Back to your first question a moment ago, though, I want to note that Jason's point about all the levels of the different layers of technology is a good one, that we need to be evolving to the next generation of technology, we need to be finding ways to make tokenization, encryption, and all these other things work, specifically for the e-commerce environment.

But today there are 1.2 billion cards circulating in the United States, most of which have 1960s-era technology in them. And later this year, when we start to see more chip cards, we are going to see early-2000s technology issued in the United States. So we aren't keeping up with the biggest area where transaction is occurring, and we need to do a better job of that.

Mr. CLAY. All right. Thank you so much for your responses.

And, Mr. Chairman, I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from North Carolina, Mr. Pittenger.

Mr. PITTENGER. Thank you, Mr. Chairman. Thank you for hosting this hearing.

And thank you to each of you for being with us today.

Governor Pawlenty, according to the Identity Theft Resource Center, financial institutions were responsible for less than 6 percent of all breaches in the United States in 2014.

Some could draw a connection with this fact and the fact that financial institutions have been subject to the Gramm-Leach-Bliley Act since 1999. Do you think this is a fair connection to make?

Mr. PAWLENTY. Congressman, I do. I don't think there would be much dispute that the financial services sector has the best cyber defenses, cyber capabilities, and most resiliency in this space. But, as everyone in this room knows, even financial institutions get breached. But, relative to other sectors, we are more advanced and get breached less.

So that is not a bragging point; it is just a point of, well, what caused that? It is caused by investment, hard work, and technology. And I do believe that Gramm-Leach-Bliley set a standard and people tried to adhere to the standard. Plus, we get examined by our regulators to that standard. And I would say that contributed to the state of the industry's cyber defenses and the relatively good quality of it.

Mr. PITTENGER. Thank you.

Yes, sir, Mr. Dodge?

Mr. DODGE. Congressman Pittenger, I would note that the Verizon report, the annual Verizon cybersecurity report, is sort of considered to be the gold standard for cyber reporting. And it found that last year there were 2,100 data loss cybersecurity intrusions. Of that, 277—

Mr. PITTENGER. You mentioned that.

Mr. DODGE. —were financial institutions, and 167 were retail businesses. There are 1,000 times more retailers operating in the United States.

So I don't think we should have the philosophy that a single regulation can guide us to a successful cybersecurity—

Mr. PITTENGER. Mr. Dodge, let me build on that. Building on Chairman Neugebauer's statement earlier and the reference to legislation, it says, "to develop, implement, and maintain a comprehensive information security program that ensures security and confidentiality of the sensitive information that is appropriate to the size, scope, and sensitivity of this information."

This was written to create some measure of flexibility so the standards are modified in ways. Do you think this is a good approach, in terms of creating these flexibilities of standards?

Mr. DODGE. We applaud Congress for looking at lots of ways to address this issue.

I think what is important is that we look at the regulatory environment as it exists today and recognize that the Gramm-Leach-Bliley Act was written specifically for the financial services commu-

nity and that there is a very strong regulatory regime that applies to most of the rest of the business community, and that is enforced through the FTC.

The FTC has moved aggressively on this over the last decade, and they have established a clear and strong set of standards that businesses have to comply with. We think that is the way to go—

Mr. PITTENGER. Let's refer to this. The provision of the bill says, "A covered entity's information security program shall be appropriate to the size and complexity of the covered entity, the nature and scope of the activities of the covered entity, and the sensitivity of the consumer's financial information to be protected."

What other flexibilities do you see would be needed that would ensure that consumers are protected but not prevent adaptability for new future threats?

Mr. DODGE. The language that you cite is not dissimilar from what we have endorsed for authority to the FTC. We think that businesses need to have a clear understanding of what their obligations are, and that the enforcement agency, as the FTC does today, has the ability to evolve their interpretation of that law over time to meet new threats, and that businesses of different sizes and businesses that collect different kinds of data should be treated based on their size and the kind of information—

Mr. PITTENGER. And this legislation seeks to do that; isn't that right?

Mr. DODGE. Based on what you quoted, that sounds right. But, as I said, we believe that you need to look at the regulatory environment as it exists today and work within that.

The debate here today is about how do we pass a law that could provide businesses with more clarity and the ability to evolve with the threat. I don't think that the objective should be to shoehorn a law that was written for one industry to apply to the entire business community. We should—

Mr. PITTENGER. And I don't think that is what this law does, according to what I just read. I think it clearly states that the provisions in there would reflect the size, complexity, the nature and scope. It personalizes it. It creates that flexibility.

Mr. DODGE. And I appreciate your focus on that, because we agree with the need for that flexibility. We simply are looking at the proposal in its entirety, and it is hard to separate things out without talking about how it would affect it when it is all merged together.

Mr. PITTENGER. Thank you.

I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Massachusetts who did not steal Mr. Mulvaney's credit card in his hypothetical, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. I appreciate that.

I want to thank the witnesses for your testimony.

Ms. Moy, on the question of Federal preemption, when we talk about complete Federal preemption, we are talking about a Federal standard, and, at least as far as this legislation goes, we are talking about Federal enforcement, as well, that is being taken away from the attorneys general of the States.

And, even further, it looks like the notification for breach will be taken away from the FEC and given to the FTC. So we are consolidating that, as well.

And, as well, it might involve, if I am—I am not sure if I am getting this correct. If we have a Federal standard, and a retailer or a business complies with that Federal standard, does that imply some type of immunity for that individual retailer? If they are complying with what the Feds require, is that also holding them harmless from any liability?

Ms. MOY. I'm sorry. You mean in an environment where this creates a floor and not a ceiling and States continue to have—

Mr. LYNCH. This would be a complete obliteration. This would be—

Ms. MOY. Right.

Mr. LYNCH. —just total preemption so you will have one standard. You could call it—well, it would be a ceiling. It would be a ceiling.

So is that implying some type of immunity or protection from liability for the complying company?

Ms. MOY. Yes, a company would then only be liable as it would be held liable under the Federal law, and any additional obligations of the State law that had previously existed would no longer be actively enforced against them.

Mr. LYNCH. Right. And, under this legislation, that would be problematic, because, as your testimony indicated, it only recognizes financial harm, right? There is a trigger—actually, personal—there is a financial harm trigger, and I think there is also a trigger for a very narrow set of personal information.

Ms. MOY. Actually, I am not sure if there is. I was under the impression that the financial harm trigger applies to everything, but perhaps you are right. I will take a look at that and—

Mr. OXMAN. If I may, Congressman—

Mr. LYNCH. Sure.

Mr. OXMAN. —the provisions of the bill, of H.R. 2205, also provide for triggers related to identity theft as well as financial harm.

Ms. MOY. Right. Yes, although many States, as I noted in my written testimony, have either no harm trigger at all, recognizing that consumers want to be notified of the breach of certain classes of information and want to be able to safeguard that information regardless of whether or not it could be used for identity theft or financial harm, and a clear majority of States have either no trigger or a trigger that is broader than just financial in nature.

Mr. LYNCH. One of the problems I have is that this introduces a Federal standard and it takes out the States. Massachusetts happens to have a very robust consumer protection privacy framework that I think will be harmed.

And we also have—we have been blessed with attorneys general who have been very active in defending consumers. And some of those cases, as you pointed out—I think the average case of breach in Massachusetts—we had 2,400 last year, but the average size was about 74 consumers. So that is not the type of thing that the FTC is going to go after, in my opinion.

Ms. MOY. That is right. And that is why we think it is so critically important—if we want to ensure that all consumers are pro-

tected by a Federal standard, it is really important that we have as many people keeping an eye on what is happening with breaches and working with companies to help develop their security standards and working with consumers to respond after their information has been breached and to watch out for potential harm that could be coming down the pike. It is really important to have the involvement of the State AGs in all of that.

Mr. LYNCH. And if we did introduce—and I am in favor of introducing a very high floor across-the-board that I think would subsume maybe close to 40 States. But I would like to have that flexibility for States that—number one, they are more flexible. Congress is not known for its speed at all. And so having the States out there with the ability to provide additional protections, especially in the face of the sophistication of some of these hackers, is very, very important, in my mind.

There is some incongruity in this bill. It talks about a Federal standard, but then it says every covered entity will be responsible for adopting a system of security protection that is commensurate with their size and their complexity. The gentleman from North Carolina just brought this up in a different context.

But how do we deal with that, where a pizza shop, a coffee shop, a bank—well, banks are a different class—but each and every company is going to be able to right-size the level of protection, but, in reality, that stream of information that is breached may not be compartmentalized?

Ms. MOY. I'm sorry. What do you mean by the information may not be compartmentalized?

Mr. LYNCH. If they hack into, as you said, your email and your password, that opens up a whole other door of information that they can access that might not be readily evident, based on where they entered the stream of information.

Ms. MOY. Right.

May I just respond to him?

Chairman HENSARLING. A very brief answer.

Ms. MOY. Sure.

Yes, I would just say there are certainly log-in credentials that, because people recycle passwords, can be used across accounts. And that is an important reason for—

Mr. LYNCH. All right. Thank you.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from California, Mr. Royce, chairman of the House Foreign Affairs Committee.

Mr. ROYCE. Thank you, Mr. Chairman.

There has been a lot of discussion here about the current liability, what it looks like. I guess one of the questions is what it should look like.

And if I could ask Governor Pawlenty—I had a question here. When a data breach occurs, how should we allocate financial responsibility for that breach?

For example, if a breach of sensitive customer information occurs at a financial institution and it is shown that the institution did not protect the customer information, as Gramm-Leach-Bliley requires, do you agree that the financial institution should be responsible for the cost of the breach?

Mr. PAWLENTY. Congressman Royce, yes. We believe that the entity that was negligent, or entities, plural, should be responsible for their negligence.

Mr. ROYCE. Okay. Then, Governor, should the same be true of the merchant? If there is a breach with a high likelihood of harm being done to the consumer, should the merchant be responsible for the costs associated with that breach to the extent that the entity has not met minimum security requirements?

Mr. PAWLENTY. Congressman Royce, absolutely.

Mr. ROYCE. And, Mr. Dodge, do you agree on that point?

Mr. DODGE. I would tell you that we do agree because that is what happens today. Today, merchants are obligated, if they have a breach, by contracts signed with the card networks to reimburse the banks for the fees associated with the costs, in addition to the fees that they pay every day every time a transaction—which is obligated to prepayment of fraud, if it happens or even if it doesn't happen. So those fees are being paid constantly.

Mr. ROYCE. So the next question I was going to ask Governor Pawlenty is: It has been proposed by some that consumers should receive notification of a data breach directly from the company that was breached even if they have no relationship with that company.

Wouldn't a simpler solution be to allow the notice to come from the company that the consumer gave their financial information to directly, while also allowing the company to identify where the breach occurred if it is known?

It is my understanding that there is currently no law, no contractual obligation that would preclude a financial institution from identifying the institution where a data breach occurred when sending out a notification to their customer. Is that your understanding, as well?

Mr. PAWLENTY. Congressman Royce, yes.

And, of course, you might imagine, if there is a breach, it unfolds in the early hours and days with a great deal of uncertainty and sense of crisis around it. So, as people think about what they are going to say publicly in sending out notices, particularly if it incriminates another company, you want to make very sure that you are articulating that correctly and accurately, for fear of liability. And so I think some companies don't name names in those initial notices over some of those concerns.

Mr. ROYCE. As we look at the cyber attacks, and we see this increasingly as we talk to European and Asian governments, a lot of these are being conducted now by state-sponsored or state-sanctioned entities. We actually, for example, see individuals traveling from a certain bureau in North Korea to Moscow to be trained, and then we see their conduct with respect to the banking system in South Korea and the attempt to implode the financial system in South Korea with those direct attacks.

What can or should be done, in the view of some of the panel here, to hold these countries accountable in situations like this? And how do we do that?

Mr. PAWLENTY. Congressman, to the extent this has evolved into an international dynamic and you have state-sponsored or semi-state-sponsored activity, the United States is going to have to re-

spond in kind at a level of country-to-country discussions and potential consequences.

As you may know, under current law, the only entity that can fire back, if you will, in cyberspace is the U.S. Government. Private entities cannot hack back. And so the deterrent or consequences for this potential behavior can only come from the U.S. Government.

And then, lastly, there needs to be rules of the road internationally. We have rogue states, semi-rookie states acting recklessly, irresponsibly, in a very concerted fashion. And what you see now in terms of payment disruption is relatively minor. The consumers get reimbursed. It is inconvenient, it is menacing, it is concerning, and you should act on that alone. But compared to some not-too-fanciful scenarios where the entire payment system is disrupted or another piece of critical infrastructure is disrupted, that is something you need to be thinking about.

Mr. ROYCE. We have seen Iranian attempts here. Have you seen that in your industry?

Mr. PAWLENTY. We are cautioned not to attribute, other than what has been reported publicly. But it has been reported publicly that North Korea was involved in an incident, an attack that was attributed to them. And I think you have seen public reports of Russian or Russian-sponsored entities, and Iranian and Iranian-sponsored entities, and on down the list.

Mr. ROYCE. Thank you very much, Governor. My time has expired.

Mr. Chairman, thank you.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from New York, Mr. Meeks.

Mr. MEEKS. Thank you, Mr. Chairman.

First, I guess, Mr. Oxman, let me ask you this question in the same line. After 9/11, we talked about having all of our intelligence agencies working closely together, et cetera. And so here, when you talk about preventing data breaches, there are a number of entities that are concerned, whether you are a device manufacturer, whether you are a network operator, whether you are a financial institution or an app developer. It seems to me that it would be important that these entities work together to develop effective mobile data protection solutions.

In your estimation, is industry working in a collaborative way, all of the interested parties, in doing that? And what, if anything, do you think that Congress can do to ensure greater collaboration so that we can make sure that everybody is working together to try to eliminate this huge problem?

Mr. OXMAN. Thank you, Congressman Meeks.

I think the good news is that the short answer to your question is yes. The industry, the ecosystem is working enormously smoothly together to deploy the next-generation security products and services that we need out there in the market to secure against these increasingly sophisticated cyber attacks.

The industry is working collectively through standards bodies, like PCI, to deploy next-generation security technologies like chip technology in cards, like tokenization to take account information

out of the system, and like encryption to secure points of entry against intrusion from cyber attacks.

The industry, as you noted, is enormously complicated. It does involve a number of different players, from financial institutions to payment processors, merchants, consumers, and device manufacturers. And as we move to new technology, like mobile payments and wearables, it is going to get even more complicated.

But, again, I think the good news is we are working very well together to deploy all these next-generation technologies because we all share an interest across the ecosystem in ensuring that our customers feel comfortable shopping at our stores and using electronic payments.

As to the second part of your question, Congressman, what can Congress do, I think H.R. 2205 represents the ideal vehicle for addressing what we do need Congress' help with, and that is unifying a patchwork of State laws that are inconsistent and, in some cases, incompatible with one another to address how we let consumers know when something does go wrong. Because criminals are sophisticated and they are going to keep acting, and we need to make sure we are all on the same page when we let our customers know if something happens. And that is where I think Congress can be helpful.

Mr. MEEKS. Thank you.

Let me ask Mr. Pawlenty, I know and you believe—in reading your testimony, you noted that the EMV chip cards have proven very effective. And I have a number of my cards now that are coming, have to switch out on them, make sure you have the chip.

But one of the questions—and this happens with my daughters, et cetera, now, that they are doing more and more shopping online. People are not going to the store as much, and they are doing shopping online. And it seems as though there is more fraud that is now taking place when people are doing this shopping online.

So can you discuss ways in which firms are innovating to prevent customers or consumers who rely more on the online shopping so that we can prevent fraud in that regard? And, again, like I asked Mr. Oxman, ways that Congress can ensure greater data breach protection as we move away from in-store purchases? It just seems that with this new generation, it is just online. My daughters won't go to stores anymore; everything is online. What can we do, in that regard?

Mr. PAWLENTY. Congressman, that is a great question. And as was mentioned earlier, the chip cards will go a long way towards eliminating or greatly reducing card-present fraud for the reasons that were mentioned earlier. So that is progress and good, and we applaud that and enthusiastically embrace it.

But as we have seen in the other EMV-adopted countries, the fraud then shifts to the online environment. And what happens, of course, is, if you make an order online, over the phone, or otherwise, you enter in your credit card number, you enter in your three- or four-digit code and your expiration date, and away you go. And so, if I have that information from you, I can make that transaction online, and it is—let's just say it is loose, to put it mildly.

So the future of that in the near term is a technology platform called tokenization, which will allow that transaction to occur with

a unique set of data that connects needed data to finalize the transaction, but the personally identifiable information isn't necessarily transmitted as part of it. It is a token, one unique signal that goes.

That is coming. It is just around the corner. And it is already into market, to some extent. But as was mentioned earlier, the cost of it is coming down, it is becoming more ubiquitous. So that will be a big part of the solution. It was invented 10 years ago. So there will be something else that will come next.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Maine, Mr. Poliquin.

Mr. POLIQUIN. Thank you, Mr. Chairman. I appreciate it very much.

And thank you, all you folks, for being here today. I really appreciate it.

Mr. Oxman, I know you and I are both from Maine, probably the safest State in America. And we invite all kinds of other folks to come up there and enjoy our State.

That being said, we are not immune to folks who are stealing our credit card numbers, or using our debit cards fraudulently, and what have you. So we know there is a problem. The problem is across the country, even in our great State of Maine.

That being said, one of the things that I have heard this morning that I am delighted about is that there seems to be some common ground, a lot of common ground, when it comes to the fact that there is an issue with cybersecurity. We all know it is there, and you folks all agree to it, even though you are from different parts of this space, if you will.

And I have also heard, if I am not mistaken, that there is a consensus that we need, instead of 48 individual laws that we have to deal with, that one national standard would be very helpful when it comes to notification.

What I would like to hear from each of you—we will start with you, Governor, if you don't mind terribly—is what else is on the top of your list. What else would you like to inform this committee about that would be very helpful for all the players in this space to make sure our consumers in Maine's Second District and throughout the country are well-protected with their bank accounts and their credit cards and what have you? What could you advise us today?

Because your members are the folks who are on the ground. You are much closer to this problem than we could ever be. Please tell us.

Mr. PAWLENTY. That is a great question. And when you think about notification, it helps notify people that there was a problem and now we need to clean up the mess.

Mr. POLIQUIN. Right.

Mr. PAWLENTY. That is little consolation for people who have the mess visited upon them. And so it is helpful.

As to standards, again, it will help as people raise their game. I think this entire space is going to evolve in a very interesting and probably disruptive fashion over the next 10 years. The things that we are talking about here today in terms of technology platforms,

as was mentioned earlier, will look very different 10 years from now. I don't think we are going to be walking around with pieces of plastic and PINs. The whole thing is shifting increasingly to mobile and other ways to make payments.

So I would say it is going to come from the technology sector, big changes and good changes.

Mr. POLIQUIN. Mr. Dodge?

Mr. DODGE. I am glad some attention is being paid to collaboration, because I think that is an important outcrop from these catastrophes, this focus.

Last year, we collaborated with the Financial Services Roundtable and the Electronic Transactions Association, with a whole bunch of merchant and financial services associations, to talk about these challenges, and to try to find some common ground.

Collaboration has also found its way into the threat-information-sharing world, where businesses can share threat information, sort of a rising tides—for a Maine term, “rising tides lift all ships”—the ability to see a threat, deflect it, and share with others what you saw and how you did it. That is really important. And we congratulate Congress for passing legislation on that last month.

I think one of the things that we really look towards is, how do we enhance security to the 21st Century and beyond? Card security today is weak. It needs to improve. There is a half-step on the calendar for later this year, but it is only a half-step. We need to get beyond that. And we really want to see Congress focus on that, and we certainly want to see the business community that is responsible for creating those cards focus on it, as well.

Mr. POLIQUIN. Mr. Oxman?

Mr. OXMAN. Thank you, Congressman Poliquin.

I am excited about the changes in technology that we are seeing in our industry. And I think if there were one thing for the committee to be aware of, it is that there actually is no need for an inquiry into that technology because the industry is working together to deploy it.

My first job was as a bank teller, during the summer after my first year in college, at Mechanics' Savings Bank in the heart of the Second District of Maine.

Mr. POLIQUIN. You bet.

Mr. OXMAN. And the hot technology back then in the 1980s was the ATM machine. Today, consumers can buy things with a watch. It is absolutely amazing what is happening out there.

And I think the good news from Congress' perspective is that the industry is deploying that technology safely, securely, and reliably, and we are going to get it done.

Mr. POLIQUIN. What about Apple Pay, Google Wallet, Square, these pieces of technology that are being developed much more quickly than I can understand for how to pay for the goods and services you buy online or through a mobile device? Do you see any problems coming down the road with those types of technology, or is that where it is going to go and where it should go, in your opinion?

Mr. OXMAN. Yes, I think this kind of technology is incredibly exciting, particularly because it allows us to deploy more robust security alongside.

The way to think about it is, it is a new means of implementing a payments transaction, of initiating that transaction. You are using your watch or your phone instead of a plastic card. And that watch or phone or whatever device it is has many more security capabilities to it than the plastic cards, so it is actually a good thing for consumers.

Mr. POLIQUIN. Mr. Orfei, unless here in this country we go down this path where we continue to work on this problem and find solutions to it, aren't we exposing our consumers and our families and our businesses to more cyber risk if Europe is ahead of us and other developed countries or parts of the world are ahead of us?

Mr. ORFEI. May I answer that question?

Mr. NEUGEBAUER [presiding]. Quickly.

Mr. ORFEI. I think the technology is going to evolve here, and we will have good answers. Particularly, mobile will be the future of payments.

But I think what is really key is this information-sharing effort that is in progress right now. Being able to collect that information, translate it so it is actionable intelligence, and then that will allow us to preempt attacks from organized crime, rogue states, and state-funded actors.

Mr. POLIQUIN. All right.

Thank you all very much. I appreciate it.

Thank you, Mr. Chairman. I yield back.

Mr. NEUGEBAUER. I thank the gentleman.

Now the gentleman from Georgia, Mr. Scott, is recognized for 5 minutes.

Mr. SCOTT. Yes. Governor Pawlenty, I would like you to address this, and anybody else can chime in, as well. But with the challenge for our migration of the EMV chip technology in the United States basically due by October 15th, why are U.S. consumers only now receiving the chip cards when consumers in Europe and Canada have had them for many years? Why are we behind the eight ball?

Mr. PAWLENTY. There is some unique history as it relates to how Europe got to where it is relating to technology, their telecommunications system, how they did batch processing, how that works relative to how we did it in the United States.

I think, to sum it up here, I would say the transition from what we had to what we need and where we are headed next is a very big transition. You think about the millions and millions and millions of point-of-sale terminals that would have to be chip-ready. Right now, only about 25 percent of retailers can even take a chip card. So they will have to flip over their systems, their point-of-sale systems, their backroom systems. Payment networks have to do the same; the banks have to do the same. So it is a massive transition.

Would we have benefited from it being done earlier? Probably. But we are where we are, and now we just need to get it done as quickly as possible. And all of this is highlighting the urgency of it.

Mr. SCOTT. Okay.

Now, since we have such a brain trust of cybersecurity before us in this distinguished panel, I want to shift gears for a moment. Are you satisfied and how would you describe the national security

threat to our country as a result of cybersecurity, as a national security issue? I think it is one we really, really have to deal with.

And how would you relate that, particularly when we have had attacks on our cybersecurity from China, from Russia, from Iran, from North Korea, ISIS, Al Qaeda, other terrorists. Now our military bases are being put on heightened terrorist attack alert at a level we haven't seen since 9/11.

What is it that we need to do more? And how do you address and how do you rate this threat at its present time as a national security issue?

Governor Pawlenty, or any of you?

Mr. PAWLENTY. I will say, Congressman, I would rate it as a clear and present danger. And that is why I said what I said earlier. I think, particularly for folks who are on the Republican side of the aisle, it is not as comfortable to say we are just going to do something uniform across the country, but I think this is elevated, not just the card and processing but many other aspects, to a national security issue.

We have known, identifiable threats to critical infrastructure of this country that would impair not just the economy but the health and well-being of our citizens if they are deployed to any sort of scale. And so it is a clear and present national security threat that I think needs to be addressed with that kind of urgency and that kind of seriousness and that kind of weight behind it.

Mr. OXMAN. And, Congressman Scott, it is a question that is answered largely by technology. And thank you for your leadership in taking a founding role in the Congressional Payments Technology Caucus, because technology companies, including many from the great State of Georgia, are out there deploying systems to secure networks against intrusion.

And there is no question that the payments industry is focused relentlessly on this. Because the security of networks and the reliability of networks and systems is why consumers choose electronic payments as their preferred method of engaging in commerce. And we need to make sure that remains a confident factor for consumers.

Mr. SCOTT. And, Mr. Oxman, how ready will we be? October is right around the corner. What are your expectations? Have we set that date? Is it accomplishable?

Mr. OXMAN. Yes, Congressman Scott, the migration in October to the chip cards is a date that we have set as a milestone, and it is a lot of work to do: 1.2 billion cards in consumers' wallets need to be replaced, and more than 8 million merchants in the United States need to upgrade their systems in order to accept chip cards. That is going to take some time.

Will we be completely finished by October? The answer, frankly, is, no, we won't be all done. But we will be largely there. And, most importantly, the industry is entirely unified in recognizing the importance of making this infrastructure upgrade. We are doing it. We are working together—merchants, financial institutions, payments companies, and consumers. And we are going to get it done.

Mr. SCOTT. Thank you, Mr. Chairman. I yield back.

Mr. NEUGEBAUER. I thank the gentleman.

The gentleman from Arkansas, Mr. Hill, is recognized for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman.

And I thank the panel for being with us this morning.

On Mrs. Maloney's comments about Gramm-Leach-Bliley and the impact on banks, having run a community bank for the entire history of Gramm-Leach-Bliley's existence, I do think it was flexible in the standards when it comes to examination and practice, both in scope of business and not. So I think that is something that has worked well in the financial services industry.

One question I have I would like the panel to react to is, what role does liability insurance coverage play here when you think about standards?

I know in our company we took out the coverage at the very modest premium for notification coverage, which was sort of what was recommended by the underwriters. I didn't find it very compelling or particularly useful, but in a large breach it certainly would be helpful to pay the out-of-pocket expenses.

But what is happening in the liability arena on insurance coverages for our entities beyond that? What standard are they setting when they come to underwrite a retailer—let's start with you, Mr. Dodge—about data breach. Because there is obviously a mathematical loss potential for one of your members.

Mr. DODGE. Sure. I will acknowledge at the outset that I don't claim to be an expert on cybersecurity liability insurance; however, my exposure to it offers me a little bit of perspective.

First is it is a pretty immature market, pretty new, and it is rapidly involving. And I know the Administration is working on ways to make that a more mature, more competitive market.

Many retailers are looking into, many have purchased liability insurance as it relates to cybersecurity. I don't have a number for that, but I suspect that number is growing by the day. And one of the challenges that they all face is where exactly to price it. They don't know how much to get, and they don't know if they are getting a great value for it. But they know that it is important to have, and they are working on making sure that improves over time.

But I think your point is a good one, sure.

Mr. HILL. Also, in the Verizon report that has been mentioned, only about 20 percent of those breaches are as a result of the retail and the banking industry, which means 80 percent aren't. And we haven't heard one question about that today.

Just last week, I got a letter from the Arkansas Medical Society, where over 60 physicians had their identity stolen when they filed their income tax return. They didn't know it until they went to hit "send" electronically to the IRS, and they suddenly learned they had already filed their return, which, of course, they hadn't.

So can you reflect on standards that we have talked about today for that other 80 percent that is not represented here today?

Or maybe, Mr. Oxman or Mr. Orfei, you might take that one?

Mr. OXMAN. Yes. Thank you, Congressman Hill. And I do think that is an important issue because the harm that consumers suffer from identity theft can in some circumstances be as impactful as the harm suffered from the theft of financial data.

And I think H.R. 2205 does a good job of making sure that all entities, not just retailers and financial institutions and payments companies, but all entities that have the storage or access to sensitive personal information are required to abide by the Federal standards that H.R. 2205 would put in place. And I do think that is a very important component of the bill.

Mr. HILL. Would anybody else like to add to that?

Mr. ORFEL. I think the fundamentals of the PCI standard are applicable across all vertical markets.

I also share your concern in my discussions with law enforcement that the healthcare systems, in particular, will be a next big target. Protecting that data and following adherence to the PCI standard would benefit those industries, as well.

Mr. HILL. I think it is a little odd that HIPAA—we can't even have a conversation about our aunt's health with the doctor without everybody jumping through hoops, but we obviously have healthcare data at risk. It is financial data, and this IRS situation is financial loss. I think this is a serious matter, certainly as serious as having your credit card number compromised.

So I am glad to hear you say that you have some comfort that the standards in this bill will help in this other 80 percent of the issue that we are not addressing today. Thank you.

Mr. Dodge?

Mr. DODGE. I would say that we also endorse a strong reasonableness standard, one that provides businesses with the strong expectations of what government considers to be a reasonable standard. We believe that it should be enforced by the FTC, and we have endorsed the legislation that came out of the Energy and Commerce Committee to do just that.

We think it is important, as we are addressing this issue, that we first look at the regulatory landscape as it is today and design solutions that fit within that, rather than moving a regulation design for one industry—in this case, the financial services industry—to apply to the entire rest of the economy.

Mr. HILL. Right. Thank you for that comment.

I yield back. Thank you.

Mr. NEUGEBAUER. I thank the gentleman.

And now the gentlewoman from Wisconsin, the ranking member of our Monetary Policy Subcommittee, Ms. Moore, is recognized for 5 minutes.

Ms. MOORE. Thank you so much, Mr. Chairman.

I just want to thank all of the witnesses for taking the time and for being patient with us. And I can tell you that you guys almost and Ms. Moy almost answered my questions when other Members were asking, and so I do want to apologize if things seem redundant.

Let me start with you, Ms. Moy. You talked about having a Federal standard, a floor standard. And you talked about the FTC really providing that service at this point. I guess I want your opinion or knowledge about whether or not you think the FTC is currently staffed up and resourced up enough to continue this stewardship.

How much more would it cost to do it? How many more employees do you anticipate? Or is there a necessity to create a new agency?

Ms. MOY. I apologize because I don't have those numbers for you, although I could do some research and try to help you answer that question.

I do think that the FTC is doing a pretty good job enforcing data security, specifically with the biggest cases. And at the State level, the States are active in this area, as well, also enforcing sometimes their own data security standard and sometimes a standard that they are drawing from the authority of their general consumer protection acts, their many FTC acts.

I think it is really important, though, to preserve the ability of what the States are doing, to preserve the ability of State AGs to continue to provide that important service, and to set our new standards at a level that will continue to preserve protections for pieces of information that would not be covered by the legislative proposals we have seen.

For example, in your own State of Wisconsin, the breach notification standard would extend to DNA and biometric data that is not necessarily covered by what we have seen in some legislative proposals.

Ms. MOORE. I really would like to know how much this will cost.

And in keeping with the same theme, Mr. Mulvaney was sort of going down this road about who pays for the cost of a breach. And on October 1, 2015, there is going to be a merchant liability shift.

And so we are at Gwen Moore's custard stand here, and I have just gotten my little smartphone to be able to swipe my card. How much is this going to cost me? Or do I just take risks and say, I will just take chances for a few years until I get my business up and start franchising my custard store? How much will it cost me to be compliant?

Mr. OXMAN. Congresswoman Moore, the good news is for a small business that is interested in upgrading their infrastructure, the costs are actually very low. You can get an EMV chip device from Square for \$30—

Ms. MOORE. Oh, okay.

Mr. OXMAN. —if you want to go that route, or you can get it from a payments processor for not much more. So the cost is actually very low for the merchant.

And the good news is that October liability shift date that you are talking about, if the merchant makes that small investment in the upgrade to accept chip cards, and if the card issuer has issued chip cards, then the liability for a fraudulent transaction and counterfeit card actually rests with the issuer. So the merchant is exactly the same as they would be today. As long as they have made that investment in the infrastructure, they don't have liability for a counterfeit card transaction in that scenario. So it is good news for the merchant.

Ms. MOORE. That was the answer that was escaping me this entire hearing; how much is it going to cost Gwen's custard stand to be able to do it.

Obviously, there will be a lot of costs for ATMs, and I guess that is a little bit more costly. How much will it cost to update all the ATMs?

Mr. OXMAN. Yes, the ATMs and, actually, fuel dispensaries, so gas stations—

Ms. MOORE. Right.

Mr. OXMAN. —actually have an extra 2 years to upgrade their infrastructure simply because it is pretty complicated to actually take the credit card equipment out of an ATM or out of a gas pump. So they don't have to worry about upgrading their infrastructure until October of 2017 for those two industries.

Ms. MOORE. Okay.

In my remaining time, for Governor Pawlenty, as the head of the Financial Services Roundtable, I guess I am just curious about why it has taken us so long to do this, why we are behind Europe and Canada? And you guys have testified that we are going to stay behind.

Mr. PAWLENTY. Yes. Some of the countries that went to EMV didn't have much legacy technology to begin with, so they could just jump to it as first adopters. Other countries have other histories, like the U.K., for example. In an era where telecom was really expensive, they loaded up all their transactions and processed them at the end of the day, called batch processing. So the ability to do, kind of, realtime communication via telecom had something to do with how and when things evolved.

All that being said, I think the United States has been slow to this issue, but the fact of the matter is we do see the need, obviously—everybody does—and we are moving as quickly now as possible to implement it and for good cause.

Ms. MOORE. Mr. Chairman, I realize my time has expired, but I just want to ask Governor Pawlenty, are the Vikings going to be as bad as they were last season?

Mr. PAWLENTY. Did you say the Packers? The Vikings. Well—

Mr. NEUGEBAUER. I think the big question is, how do we get some of that custard?

Mr. PAWLENTY. The Vikings are going to be better this year, Congresswoman.

Mr. NEUGEBAUER. The gentleman from Florida, Mr. Ross, is recognized for 5 minutes.

Mr. ROSS. Thank you, Mr. Chairman.

And thank you, panelists.

I can only preface my remarks by thinking back to the early 1980s when I was installing computer systems, little 16-bit processors in pharmacies across the eastern United States, and we would use a dial-up modem to update their drug prices and to process data. And then, at that time, the movie "WarGames" came out, starring Matthew Broderick, that showed how we can hack into the WOPR, the intelligence computer that started an international war game. And we have evolved today to where you go to Walt Disney World and you get a magic band you wear that has all your data, shows Disney exactly where you are, what you are doing, what ride you want to be on, all your billing information.

The evolution of technology has been a tremendous benefit to us. It has given us a path of expanding our commerce and our economy tremendously. And, obviously, it has given opportunities to give those who seek ill will against us, and that is why we are here.

One of the institutions of higher education, the University of South Florida, rests in my district. And 2 years ago they were designated by the Florida legislature to be the center of cybersecurity,

an academic program. Now, they have over 100 students seeking masters in this particular arena.

My question is, is there a great deal of cooperation between the private sector and the academic sector in trying to innovate ways to continue to fight cybersecurity? If anybody can address that?

Mr. DODGE. I would just speak up and say, I know that the retailers who have sought such partnerships have found welcome partnerships in it.

Last year, we established something called the Retail Cyber Intelligence Sharing Center. And at the core of that is a retail ISAC, but wrapped around that is an opportunity for educational opportunities. And I know that group has found great partners already in the academic community looking for ways to identify ways to bring future chief information security officers up through the ranks but also to share information so that everybody has the best skills available today.

Mr. ROSS. It would seem to me that would be a good partnership, even though I would say that well over 80 percent of our commerce in the cyber world is through the private sector.

Mr. Dodge, let me ask you this particular question, because as my colleague, Mr. Mulvaney, was asking you about who bears the cost of a fraudulent transaction, is it between the banks and the retailers? Is there not in existence any particular either expressed or implied right of indemnification between the parties that would allow that to be resolved absent statutory or legislative involvement?

Mr. DODGE. The fraud payment requirements, who pays after a breach or in the instance of fraud, is spelled out in the contracts. So the retailers are bound by those contracts, and their unwillingness to—if they violate those contracts, they risk losing the right to accept cards.

Mr. ROSS. So there is a limited negotiation, I guess, is what you are telling me in order for a retailer—if a retailer wants to accept a MasterCard, they accept all the terms and conditions without, really, negotiation.

Mr. DODGE. It is not a negotiation. You sign the contract presented to you.

Mr. ROSS. Okay.

And, Mr. Oxman, one of the things that we have talked about—you talked about very well and in depth is the EMV, the electronic MasterCard/Visa chip. Now, for some time this has been in practice in the European markets, has it not?

Mr. OXMAN. It has.

Mr. ROSS. And, just recently, had it not been for, I guess, an Executive Order, we would not be pursuing it as fast as we are in the United States.

What has been the reason for the delay of the implementation of the chip technology here?

Mr. OXMAN. The reason that chip technology is being deployed today in the United States and has been deployed already in Europe is the following: In Europe, they don't have the ability that we have here to authorize a transaction online.

When you swipe your card at the point of sale, what happens is that transaction is transmitted through a payment network to the

card issuer for a “yes” or “no” answer. And when the receipt is spit out 1.4 seconds later with a “yes” answer, it is because that transaction was authorized and approved online.

Mr. ROSS. I see.

Mr. OXMAN. In Europe, they don’t have the infrastructure to do that. The card authorizes the transaction—

Mr. ROSS. I see.

Mr. OXMAN. —which means that chip with the swipe machine isn’t going anywhere—

Mr. ROSS. It is making the decision right there.

Mr. OXMAN. It is making the decision right there.

Mr. ROSS. I see.

Mr. OXMAN. And that is why the chip infrastructure is necessary in Europe and hasn’t been necessary—

Mr. ROSS. And now we move into tokenization, which is essentially protecting the database of all the private information, and it is encoding or encrypting that particular transaction with a one-time identification, and then that allows anybody who captures that to have really nothing.

Mr. OXMAN. That is exactly right. The way the system works today, in many cases, your actual account number is transmitted.

Mr. ROSS. Right.

Mr. OXMAN. So what are cyber thieves looking for? They are looking for credit card numbers. Why do they breach retailers? Because there are tens of millions of them there.

In a tokenized environment, it takes the actual account number out of the equation, so there is nothing to steal and—

Mr. ROSS. How fast are we moving in that direction? Are we—

Mr. OXMAN. We are moving in that direction very quickly.

Mr. ROSS. So it is going to become the predominant barrier, if you will?

Mr. OXMAN. It is being ubiquitously deployed across all retail segments. Again, we have an existing infrastructure that needs to be replaced. It will take some time to get there, but we will get there. It is a great technology, and everyone is working together to make it happen.

Mr. ROSS. Good.

One last thing. I know we have talked about point-of-sale defenses predominantly today, but, after the data has been breached and then the consumer’s identity is stolen, how effective are some of these companies out there that allegedly protect consumers from having their identity stolen? Is that good, or is it bad, or is it just somebody else’s opportunity?

Mr. DODGE. I can’t speak to any one of those companies. I think, again, everybody needs to be vigilant. You need to monitor yourself in addition to services you may provide.

But I want to go back to a point you made a second ago, which is about advancing to the technology in cards to get to where we are in Europe and have been in Europe for a decade. The migration that is happening in the United States is only a half-step. We are only instituting a chip; we are not requiring a PIN.

Mr. ROSS. Right.

Mr. DODGE. A PIN authenticates the cardholder, and we believe that there is a redundancy. It is a belt-and-suspenders approach to

security that is needed in the card. It has worked in Europe. It has worked in Canada. It has brought fraud down. And so we should have it here.

Mr. ROSS. So PIN and the chip eliminated almost—

Mr. DODGE. You need to have it together. And we are not moving to that here in the United States because of decisions made by the card networks.

Mr. ROSS. Thank you.

I yield back.

Mr. NEUGEBAUER. I thank the gentleman.

And now the gentleman from Arizona, Mr. Schweikert, is recognized for 5 minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Okay. This may be a little way from the legislation that is being vetted. Mr. Oxman, from my listening, you seem to be the most technical member of the panel. Is that a fair—

Mr. PAWLENTY. Yes.

Mr. SCHWEIKERT. Yes. He says yes.

Mr. OXMAN. I guess I have been voted most technical.

Mr. SCHWEIKERT. As the Governor says, "Yes, give it to him."

Okay. Can we walk through a couple of mechanics? And, first, the philosophical box I want to work from is, if you and I wanted to design as robust a system as possible—I am not asking practical, but possible today, where I still have the use of my financial instruments, my credit cards, online, at the retailer, in any fashion it may be, what would I be doing?

Because when we sat through something in this regard a couple of years ago, we had such high hopes for the tokenization handoffs and the randomization of the designs of those tokens.

Is it token-plus? If you and I were designing a system here and making sure that, as we work on the legislation, it has enough openness to grab tomorrow's technology, what should we be doing?

Mr. OXMAN. A system designed from scratch would ensure that actual information that can be tied back to you or your account cannot be intercepted. Put another way, you would make sure that you didn't transmit actual information in a way that could be taken by somebody else and used in the same form.

That is the real goal of all of the layered security technologies that you see deployed today. It is dynamic, and it makes sure that intercepted information cannot be useful.

We haven't really talked about how the chip works in the chip card, for example. But the real difference between the chip and the mag stripe is it generates a unique dynamic security code—

Mr. SCHWEIKERT. Yes.

Mr. OXMAN. —with each transaction. So even if you intercepted the chip information or tried to create a counterfeit chip, you wouldn't know the code for the next transaction, so it would be useless to you.

So, again, does that—

Mr. SCHWEIKERT. It is the handoff.

Mr. OXMAN. Yes, designing a system from scratch would make sure that the information was dynamic and couldn't be tied back to anything, even if it were intercepted.

Mr. SCHWEIKERT. Now, is it a blend of, okay, here is my tokenization, handoff mechanics, and a biomechanic? If I am doing online, an IP algorithm behind saying, is this an IP that matches—what am I doing to make these things work?

Mr. OXMAN. Right. That is kind of the interesting thing about mobile payments, for example, which a lot of ETA-member companies, great technology companies, are moving to deploy—

Mr. SCHWEIKERT. You beat me to our last minute of conversation, but we might as well move on to that. As we all move to the mobile pay and sort of catching up with the rest of the world, is the technology in my payment systems on this, is that my future of transaction security?

Mr. OXMAN. It is a great future of transaction security, because what that mobile device has on there is the token that we were talking about earlier—

Mr. SCHWEIKERT. It could have all three. It could have the tokenization. It could have my bio data with my fingerprint.

Mr. OXMAN. Exactly.

Mr. SCHWEIKERT. And it obviously has its version of—it is, as you know, not technically an IP, but it has—

Mr. OXMAN. It is encrypted.

Mr. SCHWEIKERT. —the ability to hand over, saying, here is the device that goes with this.

Mr. OXMAN. That is right. So the future of technology that we are all working together to deploy has all of those elements to it. So it is almost as if we have an opportunity, thanks to the advances in technology, to devise that utopian system from scratch.

Mr. SCHWEIKERT. Okay.

Now, for everyone else on the panel, how do I incentivize that?

Mr. DODGE. The one point that I would make at the outset is, Jason is absolutely right, the future of payments is in mobile technology, and we are going there, but we are not there yet. There are 1.2 billion cards circulating in the United States, and we need to make sure we are locking down that before we move to the next generation or while we are moving to the next generation.

But I think I won't try to wade into the deep technological comments, but we believe that tokenization is a great opportunity and a great, great potential. And, certainly, mobile technology and the encryption that is in place today I think will work for a long period of time.

Mr. ORFEL. So the end game, really, is you devalue the data so that it is useless in the hands of criminals. And the three technologies that we have talked about today do exactly that: EMV at the point of sale; point-to-point encryption; and tokenization. If you bundle those correctly, and you implement it properly, the value is useless. There is no reason to break in. And even if you did, whatever you stole, you can't use anywhere else.

Mr. SCHWEIKERT. Okay.

Much of today's conversation was, who holds the liability, who pays. And my fear, at one level, is that is an absurd conversation to have. We should be having the conversation of, how do we build the robust technology so we don't have the problem?

Mr. PAWLENTY. Congressman, I know we are out of time. The good news is, it is happening. While mobile payments and some of

the things you mentioned are a small part of the picture, the rate at which they are growing is rapid, and the adoption rate, particularly for younger people, is very high. So the future that you are foreshadowing is unfolding.

Mr. SCHWEIKERT. I yield back, Mr. Chairman. Thank you.

Mr. NEUGEBAUER. I thank the chairman.

And now the gentleman from Indiana, the chairman of the Republican Policy Committee, Mr. Messer, is recognized for 5 minutes.

Mr. MESSER. I thank the panel for being here. Thank you for your stamina. I think we are getting close to wrapping up.

I wanted to talk a little bit further about breach notification, and I think, Mr. Dodge, a couple of times you got pretty close to this, but I just want to make sure I better understand your position and your organization's position.

You stated earlier that you wanted clarity for the business community, and I know you support the one sentence standard that was based on reasonableness found in the Energy and Commerce Committee bill.

Now, I think if you look at Section 4 of H.R. 2205, it has a set—a process that is laid out that, frankly, is much clearer and I think more scalable. It is based and modeled off of what banks have been doing for 16 years under Gramm-Leach-Bliley.

Can you explain from your perspective why you believe H.R. 2205's clarity isn't sufficient?

Mr. DODGE. The Gramm-Leach-Bliley Act, and certainly the legislation you are referencing, were designed primarily for the financial services industry. It was passed in 1990, 2000, and enforced over the last 15 years.

What we have argued is that you have to look at the regulatory landscape as it is today and look at what has been done for regulations that apply to other industries. And there has been a substantial body of work done by the Federal Trade Commission in enforcing cybersecurity expectations of businesses. That has established a decades-worth of case law that merchants or businesses all under the authority of the FTC understand what the expectations are of them.

Mr. MESSER. So am I hearing you say that while the Energy and Commerce bill has a one-sentence standard, you believe that one sentence incorporates the FTC standards that have been—

Mr. DODGE. I do. And I think any business that would be forced to comply with it—and most businesses today are—don't look at the sentence that would be in the legislation, but they would look at what the body of work is and the requirements that would be—

Mr. MESSER. Okay. And so that I make sure I understand your objection, is your objection to who the regulator would be? That you believe under the Energy and Commerce bill, it would be a different regulator?

Mr. DODGE. We think the way that the Energy and Commerce bill is structured and how it builds upon the work that has been undertaken by the FTC to date, it makes sense, and we believe that is the best way to move the ball forward in terms of cybersecurity.

Mr. MESSER. Okay. Other members of the panel, I don't know if anybody would like to comment on the specificity and clarity of the language in the—

Mr. PAWLENTY. Congressman, I would say while we recognize the brevity of it, to simply say, "Hey, go act reasonably," that is just a negligence standards that is built into common law for everything. We are all under a duty to go act reasonably in our daily lives and not be negligent. So it doesn't—when you are facing a threat of this magnitude, this nature, which is exponentially accelerating, to have the Congress say, "Hey, act reasonably," I think is underwhelming as a standard and expectation as we enter the age of cyber battles.

Mr. MESSER. Yes. I would agree, Governor, particularly when you have a road map that has worked for 16 years in another industry that you can lean on.

But, moving on to another topic, I would like to talk a little bit about how unreasonable delay works in the real world. There is talk about whether a notice should be immediate. Could you put some specific timeframe on when a reasonable notice would occur? Could anyone on the panel comment on whether it is realistic to require a company to notify consumers within a specific number of days?

Mr. OXMAN. I think that the challenge of the existing State laws is that different States have different requirements for what "reasonableness" means. And, obviously, all of us in the industry across the payments ecosystem and retail share an interest in making sure our customers know what happened as quickly as possible, but in some circumstances, there are issues that arise. For example, law enforcement may ask that we delay notification because they are pursuing the criminals, and they don't want to interfere with the investigation or the possibility of apprehension. So I do think that kind of flexibility is important, Congressman, because there are circumstances in which what one may think is reasonable someone else may decide—

Mr. MESSER. And is that relatively unanimous on the panel?

Ms. MOY. I would just add that I think one of the problems with having a harm trigger and having a risk analysis between the discovery of the breach and notification of the consumers is that it can delay notification to the consumers. One of the reasons that that many States have no trigger at all is to ensure that consumers get notification as quickly as possible.

Mr. MESSER. And in my very limited time, could anybody talk about over-reporting? It seems to me one of the challenges of what happens in the practical world when you have this big patchwork of standards is companies go out and over-report and there are consequences to consumers of that as well.

Ms. MOY. Once again, I would just turn to what the State AGs are saying on this topic, which is that in their conversations with consumers, they are not hearing that consumers want to hear less about breaches of their personal information. Consumers are upset about the fact that they are hearing about so many breaches because they are upset that so many breaches are taking place. But they don't want to forego the possibility of protecting themselves in the event of a breach.

Mr. MESSER. They want to be notified when they should be notified if there is a real problem.

Mr. OXMAN. I think that is right. That is fair.

Mr. MESSER. Okay. Thank you very much.

Mr. PAWLENTY. Congressman, on that last point, we do see in the auto-manufacturing recall space dealers and others noticing people paying less attention, unfortunately, to recall notices because they think they get too many of them or they are not serious enough. So they are just something to at least keep an eye on.

Mr. MESSER. Okay. Thanks, Governor.

Mr. NEUGEBAUER. I thank the gentleman.

I would like to thank our witnesses for their testimony today. It has been a little 3-hour exercise here. We appreciate your patience, but also I think the panel has been very informative. This is a very important issue to our country. It is a very important issue to the Americans that use the system on a daily basis, that we give them the confidence that they can continue to use one of the most aggressive and progressive payment systems in the world.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

With that, this hearing is adjourned.

[Whereupon, at 1:05 p.m., the hearing was adjourned.]

A P P E N D I X

May 14, 2015

FINANCIAL SERVICES COMMITTEE

**“PROTECTING CONSUMERS: FINANCIAL DATA
SECURITY IN THE AGE OF COMPUTER HACKERS”**

MAY 14, 2015

**RAYBURN 2128
10:00 AM**

**CONGRESSMAN RUBEN E. HINOJOSA’S OPENING
REMARKS FOR THE RECORD**

**THANK YOU CHAIRMAN HENSARLING AND RANKING
MEMBER WATERS FOR HOLDING THIS IMPORTANT HEARING
TODAY AND THANK YOU TO OUR PANELISTS FOR YOUR
TESTIMONY.**

**BEFORE GETTING INTO THE MATTER AT HAND, I WOULD LIKE
TO TAKE A BRIEF MOMENT TO COMMENT ON ANOTHER
CRUCIAL ISSUE BEFORE THIS COMMITTEE – THE
REAUTHORIZATION OF THE EXPORT IMPORT BANK.**

THE EXPORT-IMPORT BANK IS A VITAL FREE MARKET ECONOMIC ENGINE FOR OUR COUNTRY. NOT ONLY HAS THE BANK CONTRIBUTED TO A RESURGENCE IN AMERICAN MANUFACTURING, IT HAS HELPED CREATE AND SUSTAIN MILLIONS OF AMERICAN JOBS.

IN MY SOUTH TEXAS DISTRICT ALONE, THE BANK HAS SUPPORTED OVER 2,600 JOBS OVER THE LAST 5 YEARS. THESE ARE GOOD JOBS IN A VERY HIGH-NEED AREA THAT WOULD NOT HAVE BEEN POSSIBLE WITHOUT THE BANK. JUST THIS FEBRUARY, THE BANK FINANCED OVER \$800,000.00 WORTH OF EXPORTS IN MY DISTRICT. IN MY STATE OF TEXAS, THE BANK HAS HELPED OVER 1,000 DIFFERENT COMPANIES FINANCE \$19 BILLION DOLLARS IN EXPORTS.

CONTRARY TO THE MANY ASSERTIONS MADE AGAINST THE BANK, THE BANK IS AN UNBRIDLED, MARKET-DRIVEN SUCCESS STORY WHICH HAS LONG ENJOYED BIPARTISAN SUPPORT, AND THE SUPPORT FROM BOTH UNIONS AND BUSINESS ALIKE.

OPPOSITION TO THE EXPORT-IMPORT BANK IS ROOTED IN MISGUIDED IDEOLOGY, NOT FACTS.

THE EXPORT-IMPORT BANK HAS PROVIDED AMERICAN TAXPAYERS WITH A PROFIT OF NEARLY \$7 BILLION DOLLARS, AND THE CBO ESTIMATES THE BANK WILL GENERATE AN ADDITIONAL \$14 BILLION IN PROFIT FOR THE US TREASURY OVER THE NEXT 10 YEARS.

BANK DOES NOT PICK WINNERS AND LOSERS. THE BANK LEVERAGES PRIVATE SECTOR LENDERS IN 98% OF ITS FINANCING AND ITS FINANCING DECISIONS ARE BASED ON MARKET-DRIVEN DEMAND. UNFORTUNATELY, IT WILL BE *THIS* CONGRESS WHO PICKS WINNERS AND LOSERS IF WE DO NOT REAUTHORIZE THE BANK; AND THE WINNERS WILL BE OUR FOREIGN COMPETITORS WITH ACCESS TO LARGER AND BETTER-FUNDED EXPORT CREDIT AGENCIES.

WE SHOULD LET THE HOUSE VOTE ON THE REAUTHORIZATION OF THE BANK.



1700 N. Moore Street, Suite 2250, Arlington, VA 22209
Phone: (703) 841-2300 Fax: (703) 841-1184
Email: info@rila.org Web: www.rila.org

TESTIMONY OF

BRIAN A. DODGE, EXECUTIVE VICE PRESIDENT,
COMMUNICATIONS AND STRATEGIC INITIATIVES

RETAIL INDUSTRY LEADERS ASSOCIATION

BEFORE THE

HOUSE COMMITTEE ON FINANCIAL SERVICES

HEARING ON

“PROTECTING CONSUMERS: FINANCIAL DATA SECURITY IN THE AGE OF
COMPUTER HACKERS”

May 14, 2015

Chairman Hensarling, Ranking Member Waters and Members of the Committee, my name is Brian Dodge and I am the Executive Vice President of Communications and Strategic Initiatives at the Retail Industry Leaders Association (RILA). Thank you for the opportunity to testify today about data breach legislation and the steps that the retail industry is taking to address this important issue as well as our broader efforts to guard against cyber-attacks and protect consumers. Retailers appreciate Congress’ leadership in seeking to find a sensible path to federal data breach legislation.

RILA is the trade association of the world’s largest and most innovative retail companies. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together are responsible for more than \$1.5 trillion in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

Retailers embrace innovative technology to provide American consumers with unparalleled services and products online, through mobile applications, and in our stores. While technology presents great opportunity, nation states, criminal organizations, and other bad actors also are using it to attack businesses, institutions, and governments. As we have seen, no organization is immune from attacks and no security system is invulnerable. Retailers understand that defense against cyber-attacks must be an ongoing effort, evolving to address the changing nature of the threat. RILA is committed to working with Congress to give government and retailers the tools necessary to thwart this unprecedented attack on the United States (US) economy and bring the fight to cybercriminals around the globe.

Key Cybersecurity Issues for Retailers

As leaders in the retail community, we are taking new and significant steps to enhance cybersecurity throughout the industry. To that end, RILA formed the Retail Cyber Intelligence Sharing Center (R-CISC) in 2014 in partnership with America's most recognized retailers. The Center has opened a steady flow of information sharing between retailers, law enforcement and other relevant stakeholders. The R-CISC recently hired its first Executive Director and selected the Financial Services Information Sharing and Analysis Center (FS-ISAC) to provide a cyber threat sharing platform. The R-CISC portal will substantially increase the efficacy of the information sharing already underway by contextualizing, prioritizing and cataloging the information shared between retailers, other industries and law enforcement. These efforts already have helped prevent data breaches, protected millions of American customers and saved millions of dollars. The R-CISC is open to all retailers regardless of their membership in RILA.

For years, RILA members have been developing and deploying new technologies to achieve pioneering levels of security and service. The cyber-attacks that our industry faces change every day and our members are building layered and resilient systems to meet these threats. Key to this effort is the ability to design systems to meet actual threats rather than potentially outdated cybersecurity standards that may be enshrined in law. That is why development of any technical cybersecurity standards beyond a mandate for reasonable security must be voluntary and industry-led such as the standards embodied in the National Institute of Standards and Technology Cybersecurity Framework.

One area of security that needs immediate attention is payment card technology. RILA members have long supported the adoption of stronger debit and credit card security protections. The woefully outdated magnetic stripe technology used on cards today is the chief vulnerability in the payments ecosystem. This 1960s era technology allows cyber criminals to create counterfeit cards and commit fraud with ease. Retailers continue to press banks and card networks to provide US consumers with the same Chip and PIN technology that has proven to dramatically reduce fraud when it has been deployed elsewhere around the world. According to the Federal Reserve, PINs on debit cards make them 700 percent more secure than transactions authorized by signature.¹ While retailers are estimated to be investing more than \$8.6 billion to upgrade card terminals to accept chip cards by later this year, the new cards will be issued without PIN numbers, instead relying on only a signature to authenticate the cardholder.² Chip and signature technology falls woefully short of providing American consumers with same level of security provided to consumers in Europe, Canada and everywhere else in the developed world.

Retailers believe that American consumers deserve the best available card security and that deploying the two-factor authentication enabled through chip and PIN will prevent criminals from duplicating cards with ease, devaluing the data that retailers collect at the point of sale and ultimately reducing cyber-attacks on retailers.

¹ Federal Reserve, *2011 Interchange Fee Revenue, Covers Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions*, March 5, 2013.

² Reuters, *Retailers face \$8.65 billion bill for new generation of credit cards* (March 3, 2015), available at <http://fortune.com/2015/03/03/retailers-face-8-65-billion-bill-for-new-generation-of-credit-cards/>.

Increasing cyber threat information sharing also is vital to defeating sophisticated and coordinated cyber actors. RILA strongly supports cybersecurity information sharing legislation that provides liability protections for participating organizations. RILA applauds the House for passing H.R. 1560, the Protecting Cyber Networks Act, which is designed to strengthen law enforcement and private sector sharing to together address the growing threat of cybercrime and calls on the Senate to quickly take up and adopt H.R. 1560's flexible approach to electronic sharing. RILA also supports legislation that increases funding for government sponsored research into next generation security controls, and enhanced law enforcement capabilities to investigate and prosecute criminals internationally. The cyber-attacks faced by every sector of our economy constitute a grave national security threat that must be addressed from all angles.

Data Breach Costs to Retailers

For retailers there are many costs associated with a data breach. In the hyper competitive retail industry customers have many options when they shop. A data breach can undermine important customer trust and cost the retailer business well into the future. Further, retailers face many defined costs. Merchants are contractually obligated to compensate card issuers for losses following a data breach where cards may have been compromised in multiple ways. First, a portion of the fees retailers pay every time a card is swiped goes towards pre-paying fraud losses (even if no actual fraud occur). These swipe fees total some \$50 billion annually. Second, following a data breach retailers pay for a portion of the cost of reissuing a card, and any corresponding fraud that may have occurred, based upon a formula that every card issuer agrees to by contract with Visa and MasterCard. Card issuers are compensated for card reissuance costs even if no fraudulent activity has actually occurred on the account. For example, MasterCard reimburses card issuers on the following schedule for card reissuance:³

Reimbursement Rate Per Tier

Tier	Issuer— Gross Dollar Volume	Mag Stripe	Chip ²	PayPass	Combo ²
1	0-200 MM	USD 2.69	USD 3.66	USD 3.44	USD 4.04
2	201 MM-1 B	USD 2.31	USD 3.29	USD 3.06	USD 3.66
3	> 1B	USD 2.00	USD 2.98	USD 2.75	USD 3.35

A fixed deductible of 40 percent is subtracted from the gross eligible reimbursement amount to reflect anticipated card expirations and accounts published in previous MasterCard Alerts.

The amount a card issuer is reimbursed for both card reissuance and actual fraud losses is determined by many factors, including the number of cards requiring reimbursement, the incremental fraud associated with each individual card, the age of the card and when it was due for reissuance, etc. Visa and MasterCard privately negotiate and set these compensation rates

³ See 6.4.1 ADC Operational Reimbursement Factors, MasterCard Account Data Compromise User Guide, July 22, 2012.

with card issuers. Unfortunately, the conversation around which party should compensate whom following a data breach misses the larger point that we need to find a way to devalue the data and have more secure payment applications so that retailers are not targets for cybercrime in the first place.

Existing Data Security and Breach Notification Laws

When attacks on consumer information are successful and will cause economic harm, retailers believe that their customers have the right to be notified as promptly as possible. Retailers also believe that they have an obligation to provide customers with information that is as accurate and actionable as possible so that they can take steps to protect themselves. To that end, RILA supports federal data breach notification legislation that is practical, proportional and sets a single national standard that replaces the often incongruous and confusing patchwork of state laws in place today. A single, clear, preemptive federal standard will help ensure that customers receive timely and accurate information following a breach. To place in context the need for preemptive federal data breach legislation, we provide below a brief overview of the significant data security and breach notification laws with which retailers currently comply.

Forty-seven states, the District of Columbia (DC), Guam, Puerto Rico and the US Virgin Islands have adopted data breach notification laws. While there are many variations across these laws, as a general matter, state data breach notification laws require notification to individuals, and under some circumstances, state law enforcement, regulators, the media, or consumer reporting agencies when there is a reasonable belief of unauthorized acquisition of or access to data that compromises the security, confidentiality or integrity of an individual's covered personal information. The majority of jurisdictions include some type of risk of harm threshold that mitigates the risk of over-notification to consumers of breach incidents. Retailers operating in each of the 51 jurisdictions, must reconcile different notice time requirements, disparate requirements regarding the content of the notice, as well as differing rules to notify the jurisdictions themselves among many other requirements. For companies operating across many jurisdictions, this fact dependent analysis must occur simultaneously, rapidly, and accurately. Retailers face a significant regulatory burden to comply with the vast number and variety of these breach notice laws.

In addition to 47 state data breach notice laws and the laws in DC and the US territories, retailers are subject to robust data security regulatory regimes relating to protections for sensitive personal information. At the federal level, the Federal Trade Commission (FTC) is the primary regulator of data security for most businesses across a wide array of industry sectors, including the retail sector. Under Section 5 of the FTC Act, the FTC has authority broadly to bring enforcement actions against companies that engage in "unfair or deceptive acts or practices in or affecting commerce."⁴ Although the FTC has not promulgated data security rules, its robust enforcement activity has collectively created a "common law" of consent decrees that tend to signal what is expected from businesses regarding the collection, use, and protection of personal information. The consent decrees usually involve non-monetary remedies requiring the implementation of comprehensive company privacy or data security programs with

⁴ 15 U.S.C. § 45(a)(1).

biennial audits for up to 20 years. The FTC can impose penalties of up to \$16,000 per violation for violations of a consent decree.

The FTC uses both its authority to prevent consumer deception and unfairness to enforce data security standards.⁵ Pursuant to its authority to prevent deceptive acts or practices, the FTC can and does bring enforcement actions against companies that have failed to comply with their data security representations and statements in their public-facing privacy policies or other disclosures. Pursuant to its authority to prevent unfair acts and practices, the FTC has pursued companies that have failed to deploy reasonable and appropriate security measures to protect the sensitive personal information they possess or handle (e.g., Social Security numbers, financial account or payment card information, and other information that can lead to fraud or identity theft) using its Section 5 enforcement power.

Since 2001, the FTC has settled at least fifty cases against businesses that it charged with failing to provide reasonable data security practices. The FTC conducts enforcement investigations with a focus on reasonableness, and has stated that “a company’s data practices must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.”⁶ Over time, the FTC’s enforcement actions and other guidance materials,⁷ have created a robust set of data security expectations applicable to businesses under its jurisdiction. The FTC expects that companies implement a comprehensive information security program containing safeguards to address administrative, physical and technical risks to personal information.

Inadequate data security measures for personal information also can lead to violations of state laws. Many state laws require businesses to do some combination of the following: (1) comply with data security rules for personal information; (2) maintain the confidentiality of Social Security numbers; and (3) securely dispose of personal data. In addition to express statutory provisions relating to data security, many states have so-called “Little FTC Acts” that also can be used by state Attorneys General to enforce against what the Attorney General deems to be unreasonable data security practices.

While retailers diligently comply with this patchwork of state data breach notice and data security laws as well as federal data security requirements, a carefully crafted federal data breach law has the potential to clear up regulatory confusion, remove conflicting rules, and better protect and notify consumers.

⁵ FTC, US Senate Banking Committee Hearing on Safeguarding Consumers’ Financial Data (2014), available at http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=e6f6163c-ae31-4091-8e7c-c10e1eebbe84.

⁶ *Id.*

⁷ See FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>.

RILA Supports Sound Data Breach Legislation

RILA supports data breach legislation that includes a number of key elements that will protect consumers and allow retailers to continue to grow and innovate in our global and interconnected economy. The first goal of a successful federal statute should be to better protect customers and reduce the state-level burden on interstate commerce. To address this goal, retailers support strong preemption of state data breach notice and data security laws. Nobody benefits from the confusing variety of data breach notification laws in forty-seven states plus the District of Columbia, Guam, Puerto Rico and the US Virgin Islands. Strong preemption is necessary to ensure that a federal law is not the fifty-second data breach law with which retailers must comply. Similarly, a federal law should not include regulatory authority to allow the FTC to change notification rules, which will undercut the goal of creating a single and predictable national breach notification standard.

The second goal of data breach legislation should be to provide timely and accurate notice to consumers. Retailers support a reasonable timeframe to provide notice. The timeframe should be triggered by the confirmation of a breach and bound by the time it takes to investigate and verify facts, as fact-based notification provides customers with proper information through which to determine what action to take. Importantly, priority should be given to law enforcement seeking to apprehend cybercriminals. Notification requirements should therefore be delayed if requested by law enforcement. Moreover, requirements as to how notice must be given should be flexible and include alternatives to allow a business to reasonably reach customers when a business does not possess contact information at the time of the breach.

The third goal of data breach legislation should be targeted and clear notice when customers face real harm. Retailers support providing reasonable notice to consumers. Notice should be provided when there is a reasonable belief that a breach has or will result in identity theft, economic loss, or harm. The majority of state laws recognize that linking notice to harm is vital to enabling customers to be vigilant and potentially take action to mitigate harm. Inundating customers with notice of every systems penetration would create a perverse outcome where customers will be less likely to pay attention to breach notices or less likely to discern between breaches that may impact them and those that have no customer impact.

The fourth goal of data breach legislation should be to require that notice be provided by the entity breached. The obligation to notify and publicly acknowledge a breach creates a clear incentive to enhance a company's data security. Directing all notice obligations to entities with first party relationships removes that important incentive. While the obligation should attach to the party breached, the law should provide flexibility for entities to contractually determine the notifying party.

The fifth goal of data breach legislation should be to avoid an overly broad scope. Retailers support a precise and targeted definition of personal information. It is important that notice and data protection occurs only when consumers face real peril from the exposure of sensitive data and need to be vigilant and potentially take action. An overly broad definition that includes harmless or publicly available data will both detract from the effectiveness of the notice (over-notifying) and chill the innovative use of data by the private sector. Differentiating between truly

sensitive data requiring more restrictive security controls and harmless data that can be used more dynamically to create the next great product, service, or customer experience is vital to retailer innovation. Sweeping harmless data into the personal information definition undermines product development and the future economic growth of 21st century retailers. Also, an overbroad definition of personal information undermines a core goal of breach notice legislation, which is to provide carefully calibrated notice allowing consumers to prevent harm. Consumers that begin to ignore important communications are powerless to mitigate harm.

The sixth goal of data breach legislation should be to protect consumer data. Retailers support a carefully calibrated reasonable data security standard. If policymakers choose to address data security, the law must be carefully calibrated to recognize existing obligations and encourage companies to adhere to leading security practices. Legislating technology and prescribing technical standards will undermine cybersecurity innovation. The rapid pace of technological change ensures the obsolescence of laws that are not technology neutral. Specific standards are best left to multi-stakeholder open standards setting organizations with the technical expertise, agility, and ability to move at Internet speed.

The final goal of data breach legislation should be to ensure fair, consistent, and equitable enforcement of a data breach law. Enforcement of the law should be consistently applied by the FTC based on cases of actual harm. Similarly, to the extent civil penalty authority is provided, this authority should be capped based on actual harm to consumers. Also, any legislation should deny a private right of action as it would undermine consistent enforcement.

We have and will continue to work with Congress to address each of the above goals.

Retailers are Committed to Protecting Customer Data and Enhancing Consumer Trust

Retailers are committed to protecting our customers through investments in cybersecurity technology and personnel, increased cyber threat information sharing through a new law and the Retail Cyber Intelligence Center, and support for sound federal data breach legislation that is practical, proportional and sets a single national standard that replaces the patchwork of state laws in place today. We are engaging with policymakers and all stakeholders to advance each of these initiatives. I thank the Committee for considering the need for preemptive data breach legislation and look forward to answering your questions.



Written Testimony of Laura Moy
Senior Policy Counsel
New America's Open Technology Institute

Before the House of Representatives Financial Services Committee

Hearing on
Protecting Consumers: Financial Data Security in the Age of Computer
Hackers

May 14, 2015

Chairman Hensarling, Ranking Member Waters, and Members of the
Committee:

Thank you for working to address data security and data breaches, and for the opportunity to testify on this important issue. I represent New America's Open Technology Institute (OTI), where I am Senior Policy Counsel specializing in consumer privacy, telecommunications, and copyright. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is New America's program dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks.

I have been invited here today to present my views as a consumer and privacy advocate. Consumers today share tremendous amounts of highly personal information with a wide range of actors both online and offline. Consumers can benefit enormously from sharing personal information, but distribution of personal information beyond its original purpose can lead to financial, emotional, or even

physical harms. In recognition of those possible harms, 47 states and the District of Columbia currently have data breach laws on the books, several states have specific data security laws, and many states also use general consumer protection provisions to enforce privacy and security.

Many states are currently doing a very good job passing and adjusting data security and breach notification laws to respond to developing threats, monitoring threats to residents, guiding small businesses, and selectively bringing enforcement actions against violators. Federal agencies, as well, are successfully enforcing the data security and breach notification authorities they currently have. Consumers would therefore be best served by a federal bill on this subject that is narrow, and that merely sets a floor for disparate state laws—not a ceiling.

But in the event that Congress nevertheless seriously considers broad preemption, the new federal standard should strengthen, or at the very least preserve, important protections that consumers currently enjoy. As this Committee considers legislative proposals for a federal data security and breach notification standard, we at the Open Technology Institute urge the consideration of several elements that could ultimately be the difference between legislation that helps consumers, and legislation that harms them.

In particular, federal legislation:

- 1) should not ignore the serious physical, emotional, and other non-financial harms that consumers could suffer as a result of misuses of their personal information,
- 2) should not eliminate data security and breach notification protections for types of data that are currently protected under state law,
- 3) should provide a means to expand the range of information protected by the law as technology develops,

- 4) should not eliminate important protections under the Communications Act for telecommunications, cable, and satellite records,
- 5) should include enforcement authority for state attorneys general, and
- 6) should be crafted in such a way as to avoid preempting privacy and general consumer protection laws.¹

1. Federal Legislation Should Address Physical and Emotional Harms that Consumers Could Suffer as a Result of Misuses of Their Personal Information

This Committee’s attention to the issue of data security and breach notification is driven first and foremost by the threat of identity theft and related financial harms. Thus the bill currently before this Committee, and other bills the Committee might consider, may allow covered entities to avoid notifying customers of a breach if they determine that there is no risk of financial harm. Such “harm triggers” in breach notification bills are problematic, because it is often very difficult to trace a specific harm to a particular breach, and because after a breach has occurred, spending time and resources on the completion of a risk analysis can delay notification. Moreover, a breached entity may not have the necessary information—or the appropriate incentive—to effectively judge the risk of harm created by the breach.

In addition, trigger standards narrowly focused on financial harm ignore the many non-financial harms that can result from a data breach. For example, an

¹ These points are closely related to concerns we have previously highlighted elsewhere. See Testimony of Laura Moy before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015, *available at* <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf>; Letter to Senators John Thune and Bill Nelson, Feb. 5, 2015, <https://cdt.org/insight/letter-to-senate-on-data-breach-legislative-proposals/>.

individual could suffer harm to dignity if he stored nude photos in the cloud and those photos were compromised. If an individual's personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some circumstances, breach could even lead to physical harm. For example, the fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life.

Many state laws recognize these various types of non-financial harms. Accordingly, 33 states and the District of Columbia either require breach notification regardless of a risk assessment, or, if they do include some kind of harm trigger, take into account other types of harms beyond the strictly financial. There is no harm trigger at all in California,² Illinois,³ Minnesota,⁴ Nevada,⁵ New York,⁶ North Dakota,⁷ Texas,⁸ and the District of Columbia.⁹ The majority of states have a trigger that turns on "harm," "misuse," "loss," or "injury" not specifically financial in nature: Alaska,¹⁰ Arkansas,¹¹ Colorado,¹² Connecticut,¹³ Delaware,¹⁴ Georgia, Hawaii,¹⁵ Idaho,¹⁶ Louisiana,¹⁷ Maine,¹⁸ Maryland,¹⁹ Michigan,²⁰

² Cal. Civ. Code § 1798.29.

³ 815 Ill. Comp. Stat. § 530/10.

⁴ Minn. Stat. § 325E.61.

⁵ Nev. Rev. Stat. § 603A.220.

⁶ N.Y. General Business Laws § 899aa.

⁷ N.D. Cent. Code § 51-30-01, 51-30-02.

⁸ Tex. Bus. & Com. Code § 521.053.

⁹ D.C. Code § 28-3852.

¹⁰ Alaska Stat. § 45.48.010.

¹¹ Ark. Code Ann. § 4-110-105.

¹² Colo. Rev. Stat. § 6-1-716.

¹³ Conn. Gen. Stat. § 36a-701b.

¹⁴ Del. Code tit. 6, § 12B-102.

¹⁵ Haw. Rev. Stat. § 487N-1.

¹⁶ Idaho Code Ann. § 28-51-105.

¹⁷ La. Rev. Stat. Ann. § 51:3074.

¹⁸ Me. Rev. Stat. Ann. tit. 10, § 1348.

¹⁹ Md. Code Ann. Com. Law § 14-3504.

Mississippi,²¹ Montana,²² Nebraska,²³ New Hampshire,²⁴ New Jersey,²⁵ North Carolina,²⁶ Oregon,²⁷ Pennsylvania,²⁸ South Carolina,²⁹ Tennessee,³⁰ Utah,³¹ Vermont,³² Washington,³³ and Wyoming.³⁴

A bill with a narrow financial harm trigger that preempts state laws that contemplate other types of harm would thus constitute a step backwards for consumers in the majority of states. To address this problem, any legislation the Committee approves should either limit preemption so as to leave room for states to require notification even in circumstances where the harm is not clear or is not financial in nature, or include a trigger provision as inclusive as the most inclusive state-level triggers.

2. Federal Legislation Should Not Eliminate Data Security and Breach Notification Protections for Types of Data Currently Protected Under State Law

Many privacy and consumer advocates are concerned about recent legislation proposals on data security and breach notification that define the protected class of personal information too narrowly. A definition narrower than

²⁰ Mich. Comp. Laws § 445-72.

²¹ Miss. Code Ann. § 75-24-29.

²² Mon. Code Ann. § 30-14-1704.

²³ Neb. Rev. Stat. § 87-803

²⁴ N.H. Rev. Stat. Ann. § 359-C:20

²⁵ N.J. Stat. Ann. § C.56:8-163.

²⁶ N.C. Gen. Stat. § 75-61; *see* N.C. Gen. Stat § 75-65.

²⁷ Or. Rev. Stat. § 646A.604.

²⁸ 73 Pa. Stat. Ann. § 2302.

²⁹ S.C. Code Ann. § 1-11-490.

³⁰ Tenn. Code Ann. § 47-18-2107.

³¹ Utah Code Ann. § 13-44-202.

³² Vt. Stat. Ann. § 2435.

³³ Wash. Rev. Code § 19.255.010.

³⁴ Wyo. Stat. Ann. § 40-12-502.

that of state data security and breach notification laws, in combination with broad preemption, would weaken existing protections in a number of states.

For example, under California's breach notification law, entities must notify consumers of unauthorized access to "[a] user name or email address, in combination with a password or security question and answer that would permit access to an online account."³⁵ Florida law also covers login information for online accounts.³⁶ Not only does coverage for online account login credentials help protect accounts holding private, but arguably non-financial, information such as personal emails and photographs, but it often protects a range of other online accounts, because many consumers recycle the same password across multiple accounts. To illustrate, consider the recent reports regarding Uber accounts that were hacked into, resulting in fraudulent charges to customers for rides they never took. Last week, reporter Joseph Cox wrote about how those accounts may have been broken into using login credentials for unrelated accounts that were disclosed in other breaches:

First, a hacker will get hold of any of the myriad data dumps of email and password combinations that are circulated in the digital underground. This list of login details will then be loaded into a computer program along with the Uber website configuration file. From here, the program will cycle through all of the login credentials and try them on the Uber website, in the hope that they have also been used to set up an Uber account.

"It's basically checking a database dump/account list against a certain website and displaying results," [a hacker who calls himself] Aaron told Motherboard over encrypted chat.

³⁵ Cal. Civ. Code § 1798.29.

³⁶ Fla. Stat. § 501.171.

Aaron then demonstrated this process, and had accessed an Uber account within minutes. He tested 50 email and password combinations sourced from a leak of a gaming website, and two worked successfully on Uber. Aaron claimed one of these was a rider's account, and he then sent several censored screenshots of the user's trip history and some of their credit card details.³⁷

A number of state laws also protect information about physical and mental health, medical history, and insurance, including laws in California,³⁸ Florida,³⁹ Missouri,⁴⁰ New Hampshire,⁴¹ North Dakota,⁴² Texas,⁴³ Virginia,⁴⁴ and—beginning later this year as recently passed bills go into effect—Hawaii,⁴⁵ Montana,⁴⁶ and Wyoming.⁴⁷ Attackers use information about health and medical care to facilitate

³⁷ Joseph Cox, *How Hackers Can Crack People's Uber Accounts to Sell on the Dark Web*, Medium (May 4, 2015), <http://motherboard.vice.com/read/how-hackers-cracked-peoples-uber-accounts-to-sell-on-the-dark-web>.

³⁸ Cal. Civ. Code § 1798.29.

³⁹ Several federal data security and breach notification legislative proposals include a carve-out for entities already covered by federal laws that govern health information privacy. However, there are entities not covered by those federal laws that collect health-related information, and several legislative proposals would preempt state laws that cover health information and extend to those entities, without providing comparable coverage under the new federal standard.

⁴⁰ Mo. Rev. Stat. § 407.1500.

⁴¹ N.H. Rev. Stat. Ann. § 359-C:20

⁴² N.D. Cent. Code § 51-30-01, 51-30-02.

⁴³ Tex. Bus. & Com. Code § 521.002.

⁴⁴ Va. Code Ann. 32.1-127.1C.

⁴⁵ See Elizabeth Snell, *Wyoming Security Breach Notification Bill Includes Health Information*, Health IT Security (Feb. 23, 2015), <http://healthitsecurity.com/2015/02/23/wyo-security-breach-notification-bill-includes-health-data/>.

⁴⁶ See Cynthia Larose, Mintz Levin, *State Data Breach Notification Law Updates* (Mar. 10, 2015), <http://www.privacyandsecuritymatters.com/2015/03/state-data-breach-notification-law-updates/>.

⁴⁷ See Snell, *supra* note 45.

medical identity theft, a rapidly growing threat.⁴⁸ Not only does medical identity theft often result in enormous charges to a patient for medical care she never received, but it can also pollute her medical record with false information about her health status, which could lead to additional complications or even physical harm down the road⁴⁹. Health and medical information can also be used to inform “spear phishing” attacks, in which an attacker posing as a medical or insurance provider sends a fake bill or email to a patient asking for billing information related to recent treatment, thus tricking the patient into providing sensitive financial information.

North Dakota’s breach notification law protects electronic signature, date of birth, and mother’s maiden name, all pieces of information that could be used to verify identity for the purpose of fraudulently creating or logging into an online or financial account.⁵⁰

Health and medical information, login credentials for online accounts, and electronic signatures are just a few important categories of private information that would not be covered by a number of federal legislative proposals we have seen this term, including the one before this Committee. At the same time, most proposals we have seen would eliminate all of the above-referenced state laws that

⁴⁸ Ponemon Institute, *Fifth Annual Study on Medical Identity Theft 8* (2015), available at <http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/>; Dan Munro, *New Study Says Over 2 Million Americans Are Victims Of Medical Identity Theft*, *Forbes* (Feb. 23, 2015), <http://www.forbes.com/sites/danmunro/2015/02/23/new-study-says-over-2-million-americans-are-victims-of-medical-identity-theft/>.

⁴⁹ See Experian, *Prevent Medical Identity Theft*, <http://www.protectmyid.com/identity-theft-protection-resources/prevention-tips/medical-benefits.aspx> (last visited May 11, 2015) (“When the victim seeks care, he or she could end up with the wrong medical history, wrong blood type, wrong allergies and other false information that could lead to serious problems. Victims may also find that their health insurance benefits have been exhausted due to a long period of misuse.”).

⁵⁰ N.D. Cent. Code § 51-30.

do protect that information, substantially weakening the protections that consumers currently enjoy. We urge this Committee not to approve such a bill.

3. Federal Legislation Should Provide Flexibility to Adjust to New and Changing Threats

Relatedly, we are concerned that a number of legislative proposals we have seen would not provide the necessary flexibility to account for changing technology and information practices. Consumers are constantly encountering new types of threats as the information landscape evolves and creative attackers come up with new ways to exploit breached data. Right now, states are doing a good job responding to developing threats affecting their residents by adjusting data security and breach notification protections as necessary. Indeed, the fact that medical information is now covered by laws in ten states—including three that just passed bills this year—signals a deliberate response to the growing threat of medical identity theft, of which an estimated 2.32 million adult-aged Americans or close family members were victims during or before 2014, an increase over 2013 of 21.7%.⁵¹

We can't always forecast the next big threat years in advance, but unfortunately, we know that there will be one. For example, there are now multiple services that allow customers to upload photographs of physical car keys and house keys to the cloud, then order copies of those keys through an app, over the Web, or at key-cutting kiosks located at brick-and-mortar stores.⁵² Will malicious attackers begin targeting photographs of keys to victims' homes? It might be too early to tell, but if they do, companies that collect and maintain that information

⁵¹ Ponemon Institute, *supra* note 48.

⁵² Andy Greenberg, *The App I Used To Break into My Neighbor's Home*, WIRED (Jul. 25, 2014), <http://www.wired.com/2014/07/keyme-let-me-break-in/>; Sean Gallagher, *Now You Can Put Your Keys in the Cloud—Your House Keys*, Ars Technica (Mar. 20, 2015), <http://arstechnica.com/information-technology/2015/03/now-you-can-put-your-keys-in-the-cloud-your-house-keys/>.

ought to notify their customers, and the law ought to be able to be quickly adjusted to make sure that they do, without Congress having to pass another bill first.

The flexibility we need could be built into federal legislation in one of two ways. First, Congress could limit preemption in a manner that allows states to continue to establish standards for categories of information that fall outside the scope of federal protection as, for example, Hawaii, Montana, and Wyoming did just this year with respect to medical information.⁵³ Alternatively, Congress could establish agency rulemaking authority to redefine the category of protected information as appropriate to meet new threats. We urge the Committee not to approve any data security and breach notification legislation that does neither of these two things.

4. Federal Legislation Should Not Eliminate Important Protections Under the Communications Act for Telecommunications, Cable, and Satellite Records

Federal legislation should not supersede important provisions of the Communications Act that protect the personal information of telecommunications, cable, and satellite customers. Under some legislative proposals, certain types of private information currently covered under the Communications Act would no longer be protected, and the information that would still be covered would be covered by lesser standards.

The Communications Act protects telecommunications subscribers' CPNI, which includes virtually all information about a customer's use of the service.⁵⁴ It also protects cable⁵⁵ and satellite⁵⁶ subscribers' information, including their viewing histories. But as with email login information and health records, some

⁵³ See Snell, *supra* note 45; Larose, *supra* note 46.

⁵⁴ 47 U.S.C. § 222.

⁵⁵ 47 U.S.C. § 551.

⁵⁶ 47 U.S.C. § 338.

bills we have seen this term—including the one currently before this Committee—are too narrow to cover all CPNI, and would not protect cable and satellite viewing histories at all. As a result, data security and breach notification protections for those types of information would simply be eliminated.

Such a reduction of the Federal Communications Commission's CPNI authority could not come at a worse time for consumers, because the FCC has just reclassified broadband Internet access as a telecommunications service under Title II of the Communications Act, enabling it to apply its CPNI authority to broadband providers. Indeed, the FCC just held a public workshop to explore issues associated with the application of the privacy provisions of Title II to broadband.⁵⁷ Applied to broadband, the CPNI provisions will require Internet service providers to safeguard information about use of the service that, as gatekeepers, they are in a unique position to collect. This could include information such as what sites an Internet user visits and how often, with whom she chats online, what apps she uses, what wireless devices she owns, and even the location of those devices.

It would not make sense to replace the strong data security and breach protections of context-specific federal laws such as the Communications Act with narrow protections designed to combat identity theft and fraud. While the primary purpose of many data security and breach notification standards is to protect consumers against financial harms, there are other important policy justifications for the data security and breach notification protections of other context-specific laws. For example, the protections of HIPAA strive to protect the relationship between medical patients and medical providers so that patients will be open and candid about their health status and needs so as to facilitate the best medical treatment possible. The protections of attorney-client privilege, as well as attorneys'

⁵⁷ FCC, *Public Workshop on Broadband Consumer Privacy* (Apr. 28, 2015), <https://www.fcc.gov/events/wcb-and-cgb-public-workshop-broadband-consumer-privacy>.

ethical obligations to keep client communications confidential, are designed to protect attorney-client relationships so that clients can be candid as they seek legal advice.

Analogously, the data security and breach notification protections of the Communications Act serve to foster citizens' confidence in our communications networks as safe places for the exercise of free and open speech and association. Disclosure of the fact that a person privately called a prenatal clinic, visited an online auction platform for firearms, or ordered an adult film on demand might not lead to financial harm, but if she did not trust that information to be maintained with the highest level of security protections, she might self-sensor her actions.

The consumer protections provided by the Communications Act are of critical importance to consumers, and appropriately overseen by an agency with decades of experience regulating entities that serve as gatekeepers to essential communications networks. Federal data security and breach notification legislation should not eliminate core components of those protections.

5. Federal Legislation Should Include Enforcement Authority for State Attorneys General

In the event the Committee ultimately approves a bill that preempts state data security and breach notification laws, the Committee should ensure that any such bill nevertheless includes both a mechanism to notify, and an enforcement role for, state attorneys general. At a minimum, state attorneys general should have the authority to bring actions in federal court under the new federal standard.

State attorneys general play a critical role in policing data security and guiding breach notification to match the needs of their own residents. In addition, state attorneys general are essential in conducting ongoing monitoring after a breach has occurred to help protect residents from any aftermath, especially where small data breaches are concerned. According to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013,

97% of which involved fewer than 10,000 affected individuals.⁵⁸ Each data breach affected, on average, 74 individuals.⁵⁹

Federal agencies are well equipped to address large data security and breach notification cases, but could be overwhelmed if they lose the complementary consumer protection support of state attorneys general in thousands of small cases each year. To ensure that consumers receive the best protection they possibly can—even when they are among a small handful of individuals affected by a small breach—state attorneys general must be given the ability to help enforce any new federal standard.

6. Federal Legislation Narrowly Designed for Data Security and Breach Notification Should Be Crafted Not to Preempt a Wide Range of Privacy and General Consumer Protection Laws

Federal legislation also must be careful not to invalidate a wide range of existing consumer protections under state law and the Communications Act, including provisions that are at times used to enforce data security, but that are also used to provide other consumer or privacy protections. For example, the preemption provisions of some legislative proposals we have seen extend only to securing information from unauthorized access,⁶⁰ but as a practical matter, it will

⁵⁸ Testimony of Sara Cable before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015, *available at* <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-CableS-20150318.pdf>.

⁵⁹ *Id.*

⁶⁰ H.R. 2205 would preempt requirements or prohibitions imposed under state law with respect to “safeguard[ing] information relating to consumers from (A) unauthorized access; and (B) unauthorized acquisition.” H.R. 1770 would preempt state law “relating to or with respect to the security of data in electronic form or notification following a breach of security.” It would supersede several sections of the Communications Act insofar as they “apply to covered entities with respect to securing information in electronic form from unauthorized access, including

be exceedingly difficult to draw the line between information security and breach notification on the one hand, and privacy and general consumer protection on the other.

Generally speaking, “privacy” has to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information “security” refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject’s privacy (his right to control how his information is used or shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Privacy and security are thus distinct concepts, but they go hand in hand. From the consumer’s perspective, a data breach that results in the exposure of her call records to the world is a terrible violation of her privacy. But the cause of the privacy violation may be a breakdown in security.

Accordingly, agencies enforcing against entities for security failures cite both privacy and security at the same time. For example, in the April 8, 2015 Order issued by the FCC adopting a Consent Decree to resolve its investigation into a data breach at AT&T, the FCC explained that “AT&T will be required to improve its *privacy* and data security practices by appointing a senior compliance manager who is *privacy certified*, conducting a *privacy risk assessment*, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company’s *privacy policies* and the applicable *privacy legal authorities*.”⁶¹ Similarly, in the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission

notification of unauthorized access to data in electronic form containing personal information.”

⁶¹ *AT&T Services, Inc.*, Order, para. 2 (2015), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf (emphasis added).

argued that Twitter had “failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information *and honor the privacy choices exercised by its users in designating certain tweets as nonpublic.*”⁶²

Not only does enforcement often address privacy and security simultaneously, but many laws that protect consumers’ personal information could also be thought of simultaneously in terms of both privacy and security. For example, in California, the Song-Beverly Credit Card Act prohibits retailers from recording any “personal identification information” of a credit cardholder in the course of a transaction.⁶³ In Connecticut, Section 42-470 of the General Statutes prohibits the public posting of any individual’s Social Security number.⁶⁴ These laws could be framed as both privacy and data security laws. State-level general consumer protection laws prohibiting unfair and deceptive trade practices (sometimes known as “mini-FTC Acts”) are also used to enforce both privacy and security.

Because each of these examples highlights a circumstance where privacy and security regulations are blended together, consumer and privacy advocates are very concerned that some legislative proposals that may intend to leave intact privacy laws could nevertheless unintentionally eliminate some more privacy-oriented consumer protections that have a data security aspect. We therefore urge the Committee to carefully tailor the scope of preemption in any data security and breach notification bill it approves to avoid invalidating numerous privacy protections.

⁶² *Twitter, Inc., Complaint*, para. 11 (2010), available at <https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twittercmpt.pdf> (emphasis added).

⁶³ Cal. Civ. Code § 1747.08.

⁶⁴ Conn. Gen. Stat. § 42-470.

Conclusion

We are not unequivocally opposed to the idea of federal data security and breach notification legislation, but any such legislation must strike a careful balance between preempting existing laws and providing consumers with new protections. The Open Technology Institute appreciates your commitment to consumer privacy, and we look forward to working with you to strengthen this bill and strike a better balance as it moves forward. I am grateful for the Committee's attention to this important issue, and for the opportunity to present this testimony.



Statement of Stephen W. Orfei
General Manager
PCI Security Standards Council

Before the Committee on Financial Services,
United States House of Representatives
Protecting Consumers: Financial Data Security in the Age of Computer Hackers
May 14, 2015
2129 Rayburn House Office Building

Introduction

Chairman Hensarling, Ranking Member Waters, members of the committee, on behalf of the PCI Security Standards Council, thank you for inviting us to testify today.

My name is Stephen Orfei and I am the General Manager of the Payment Card Industry (PCI) Security Standards Council (SSC), a global industry initiative and membership organization, focused on securing payment card data. Working with a global community of industry players, our organization has created data security standards—notably the PCI Data Security Standard (PCI DSS)—certification programs, training courses and best practice guidelines to help improve payment card security.

Together with our community of over one thousand of the world's leading businesses, we're tackling data security challenges from password complexity to proper protection of EMV Chip Terminals. Our work is broad because there is no silver bullet to securing payment card data. No single technology is a panacea; security technology is constantly evolving and requires a multi-layered approach across the payment chain.

Work by the PCI Security Standards Council demonstrates effective industry collaboration to develop private sector standards. Simply put, the PCI Standards are the best line of defense against the criminals who threaten our way of life by seeking to steal and utilize payment card data. And while recent high profile breaches have captured the nation's attention, the PCI Council has stimulated great progress over the past eight years in securing payment card data through a collaborative cross-industry approach, and we continue to build upon the way we protect this data.

We understand that consumers are upset when their payment card data is put at risk of misuse and—while the PCI Security Standards Council is not a name most consumers know—we are sensitive to the impact that breaches cause for consumers. Consumers can take comfort from the fact that many of the organizations they do business with have joined with the PCI Council to collaborate in an effort to better protect their payment card data.

Payment card security: a dynamic environment

Since the threat landscape is constantly evolving, the PCI Council expects its standards will do the same. Confidence that businesses are protecting payment card data is paramount to a healthy economy and payment process—both in person and online. That's why to date, more than one thousand of the world's leading retailers, airlines, banks, hotels, payment processors, government agencies, universities, and technology companies have joined with the PCI Council as Participating Organizations and as part of our community to develop security standards that apply across the spectrum of today's global multi-channel and online businesses.

Our Board of Advisors is a global, active, cross-industry group that includes merchants such as Starbucks, Wal-Mart, British Airways; financial institutions such as Citi and Barclaycard; technology companies such as Cisco, RSA; and service providers such as First Data.

Our community members are living on the front lines of this battle and are therefore well placed, through the unique forum of the PCI Council, to provide input about threats they are seeing and ideas for how to tackle these threats through the PCI Standards. The Council and the PCI community have the resources to continually monitor and provide updates through standards, published FAQs, Special Interest Group work, and guidance papers on emerging threats and new ways to improve payment security. Examples include updated wireless guidance and security guidelines for merchants wishing to accept mobile payments.

Now in version 3.1, the PCI Data Security Standard (PCI DSS) is our overarching data security standard, built on 12 principles that cover everything from implementing strong access control, monitoring and testing networks, to having an information security policy. During updates to this standard, we receive hundreds of pieces of feedback from our community. This is almost evenly split between feedback from domestic and international organizations, highlighting the global nature of participation in the PCI Council and the need to provide standards and resources that can be adopted globally to support the international nature of the payment system.

This feedback has enabled us to be directly responsive to challenges that organizations are facing every day in securing cardholder data. For example, in this latest round of PCI DSS revisions, community feedback indicated changes were needed to secure password recommendations. Password strength remains a challenge—as “123456” and “password” are still the most common passwords used by global businesses—and is highlighted in industry reports as a common failure leading to data compromise. Small merchants in particular often do not change passwords on point of sale (POS) applications and devices. With the help of the PCI community, the Council has updated requirements to make clear that default passwords should never be used, all passwords must be regularly changed and not continually repeated, should never be shared, and must always be of appropriate strength. Beyond promulgating appropriate standards, we have taken steps through training and public outreach to educate the merchant community on the importance of following proper password protocols.

Recognizing the need for a multi-layered approach, in addition to the PCI DSS, the Council and community have developed standards that cover payment applications, card production, PIN security, EMV Chip Terminals and other PIN entry devices. In other areas, based on community feedback, we have produced standards and guidance on other technologies such as tokenization and point-to-point encryption. These technologies can dramatically increase data security at vulnerable points along the transactional chain. Tokenization and point-to-point encryption remove or render payment card information useless to cyber criminals, and work in concert with other PCI Standards to offer additional protection to payment card data. Going forward, “de-valuing” payment card data is a key strategy for erasing the monetary incentive for cyber criminals to commit data breaches.

In addition to developing and updating standards, every year the PCI community votes on which topics they would like to explore with the Council and provide related guidance. Over the last few years the working groups formed by the Council to address these concerns have drawn hundreds of organizations to collaborate together to produce resources on third party security assurance, cloud computing, best

practices for maintaining compliance, e-commerce guidelines, virtualization, and wireless security. Other recent Council initiatives have addressed promoting security awareness by employees, ATM security, PIN security, and mobile payment acceptance security for developers and merchants. A key topic this year is daily log monitoring—a PCI DSS requirement that is critical for detecting (and stopping) early stages of a data breach in progress.

EMV Chip & PCI Standards—a strong combination

One technology that has garnered a great deal of recent attention is EMV chip—a technology that has widespread use in Europe and other regions. EMV chip is an extremely effective method of reducing counterfeit and lost/stolen card fraud in a face-to-face payments environment. That's why the PCI Security Standards Council supports the deployment of EMV chip technology.

However, global adoption of EMV chip, including broad deployment in the United States, does not preclude the need for a strong data security posture to prevent the loss of cardholder data from intrusions and data breaches. We must continue to strengthen data security protections that are designed to prevent the unauthorized access and exfiltration of cardholder data.

Payment cards are used in a variety of remote channels—such as electronic commerce—where today's EMV chip technology is not typically an option for securing payment transactions. Security innovation continues to occur for online payments beyond existing fraud detection and prevention systems. Technologies such as authentication, tokenization, and other frameworks are being developed, including some solutions that may involve EMV chip—yet broad adoption of these solutions is not on the short-term horizon. Consequently, the industry needs to continue to protect cardholder data across all payment channels to minimize the ongoing risks of data loss and resulting cross-channel fraud, such as may be experienced in the online channel.

Nor does EMV chip negate the need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees, and having clear processes for the handling of sensitive payment card data. These processes are critical for all businesses—both large retailers and small businesses—who themselves have become a target for cyber criminals. At smaller businesses, EMV chip technology will have a strong positive impact. But if small businesses are not aware of the need to secure other parts of their systems, or if they purchase services and products that are not capable of doing that for them, then they will still be subject to the ongoing exposure of the compromise of cardholder data and resulting financial or reputational risk.

Similarly, protection from malware-based attacks requires more than just EMV chip technology. Reports in the press and subsequent forensic analyses regarding recent breaches point to insertion of complex malware into vulnerable back-office computers, which were used by attackers as a gateway to POS systems containing unprotected cardholder data. EMV chip technology could not have prevented the unauthorized access, introduction of malware, and subsequent exfiltration of cardholder data. Failure of other security protocols required under PCI Standards is necessary for malware to be inserted.

Finally, EMV chip technology does not prevent memory scraping, a technique that has been highlighted in press reports of recent breaches. Other safeguards are needed to do so. In our latest versions of security standards for point of sale devices, (PCI PIN Transaction Security Requirements, or "PTS"), the Council includes requirements to further counter this threat. These include improved tamper responsiveness so that devices will cease to operate if they are opened or tampered with and the creation of electronic signatures that prevent applications that have not been "whitelisted" from being installed. Our newest version of the standard, PTS 4.0, requires a default reset every 24 hours that would remove malware from memory and reduce the risk of data being obtained in this way. By responding to the Council's PTS requirements, POS manufacturers are bringing more secure products to market that reflect a standards development process that incorporates feedback from a broad base of diverse stakeholders.

Used together, EMV chip, PCI Standards, complementary technologies and solutions such as tokenization and encryption, along with many other tools can provide strong protections for payment card

data. I want to take this opportunity to encourage all parties in the payment chain—whether they are EMV chip ready or not—to take a multi-layered approach to protect consumers' payment card data. There are no easy answers and no shortcuts to security.

Global adoption of EMV chip is necessary and important. Indeed, when EMV chip technology does become broadly deployed in the US marketplace and fraud migrates to less secure transaction environments, PCI Standards will remain critical.

Beyond PCI Standards – building a support infrastructure

An effective security program through PCI is not focused on technology alone; it includes people and process as key parts of payment card data protection. PCI Standards highlight the need for secure software development processes, regularly updated security policies, clear access controls, and security awareness education for employees. Employees have to know not to click on suspicious links, why it is important to have secure passwords, and to question suspicious activity at the point of sale. For example, "Many [retail data breach] incidents involved direct social engineering of store employees (often via a simple phone call) in order to trick them into providing the password needed for remote access to the POS," according to the *Verizon 2015 Data Breach Investigations Report*.

Most standards' organizations create standards, and no more. PCI Security Standards Council, however, recognizes that standards, without more, are only tools, and not solutions. And standards alone do not address the critical challenges of training people and improving processes.

Consequently, the Council is actively distinguishing between "point-in-time compliance" with PCI Standards and "security." Achieving an ongoing state of payment security requires continuous effort in deploying security controls, monitoring their effective use, and diligently applying daily processes and best practices. This is a challenge, as noted by the *Verizon 2015 PCI Compliance Report*: "Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place." And, "But for most companies the DSS provides a useful baseline. While validation is no assurance of security, not being compliant is pretty much a guarantee that you're not secure."

To help organizations improve continuous payment data security, the Council takes a holistic approach to securing payment card data, and its work encompasses both PCI Standards development and maintenance of programs that support standards implementation across the payment chain. The Council believes that providing a full suite of tools to support implementation and ongoing sustainment is the most effective way to ensure the protection of payment card data. To support successful implementation of PCI Standards, the Council maintains programs that certify and validate certain hardware and software products to support payment security. For example, the Council wants to make it easy for merchants and financial institutions to deploy the latest and most secure terminals and so maintains a public listing on its website for them to consult before purchasing products. We realize it takes time and money to upgrade POS terminals and we encourage businesses that are looking to upgrade for EMV chip to consider other necessary security measures by choosing a POS terminal from this list. Similarly, we are supporting the adoption of point-to-point encryption, and listing appropriate solutions on our website to take a solutions-oriented approach to helping retailers more readily implement security in line with the PCI standards.

Additionally, the Council runs a program that develops and maintains a pool of global assessment personnel to help work with organizations that deploy PCI Standards to assess and sustain their performance in using PCI Standards. The Council also focuses on creating education and training opportunities to build expertise in protecting payment card data in different environments and from the various viewpoints of stakeholders in the payment chain. Since our inception, we have trained tens of thousands of individuals, including staff from large merchants, leading technology companies and government agencies. Finally, we devote substantial resources to creating public campaigns to raise awareness of these resources and the issue of protecting payment card data.

The PCI community and large organizations that accept, store, or transmit payment card data worldwide have made important strides in adopting globally consistent security protocols. However, the Council recognizes that small organizations remain vulnerable. Smaller businesses lack IT staff and budgets to devote resources to following or participating in the development of industry standards. But they can take simple steps like updating passwords, firewalls, and ensuring they are configured to accept automatic security updates. Additionally, to help this population, the Council promotes its listings of validated products, and recently launched a program, the Qualified Integrator and Reseller program (QIR) to provide a pool of personnel able to help small businesses ensure high quality and secure installation of their payment systems.

The work of the Council covers the entire payment security environment with the goal of providing or facilitating access to all the tools necessary—standards, products, assessors, educational resources, and training—for stakeholders to successfully secure payment card data. We do this because we believe that no one technology is a panacea and effective security requires a multi-layered approach.

Public – private collaboration

The Council welcomes this hearing and the government's attention on this critical issue. The recent data breaches underscore the importance of constant vigilance in the face of threats to payment card data. We are hopeful that this hearing will help raise awareness of the importance of a multi-layered approach to payment card security.

There are very clear ways in which the government can help improve the payment data security environment. For example, government can champion stronger law enforcement efforts worldwide, particularly due to the global nature of these threats. It can also encourage stiff penalties for cybercrimes to act as a deterrent. Also, there is much public discussion about simplifying data breach notification laws and promoting information sharing between public and private sectors. These are all opportunities for the government to help tackle this challenge.

The Council is an active participant in government research in this area: we have provided resources, expertise and ideas to FS-ISAC, NIST, DHS, and the Secret Service, as well as global agencies such as Interpol and Europol. We remain ready and willing to do more.

Twenty years ago, through its passage of the Technology Transfer and Advancement Act of 1995, Congress recognized that government should rely on the private sector to develop standards rather than to develop them itself. The substantial benefits of the unique, U.S. "bottom up" standards development process have been well recognized. They include the more rapid development and adoption of standards that are more responsive to market needs, representing an enormous savings in time to government and in cost to taxpayers.

The Council believes that the development of standards to protect payment card data is something the private sector, and PCI specifically, is uniquely qualified to do. It is unlikely any government agency could duplicate the expansive global reach, expertise, and decisiveness of the PCI Council. High profile events such as the recent breaches are a legitimate area of inquiry for the Congress, but should not serve as a justification to impose new government regulations. Any government standard in this area would likely be significantly less effective in addressing current threats, and less nimble in protecting consumers from future threats, than the constantly evolving PCI Standards.

Conclusion

In March, the *Verizon 2015 PCI Compliance Report* said: "Of all the data breaches that our forensics team has investigated over the last 10 years, not a single company has been found to be compliant at the time of the breach—this underscores the importance of PCI DSS compliance."

But we recognize that compliance is not the endgame. Security is. That's why it's so critical that companies maintain this effort through ongoing vigilance.

Recent breaches at retailers underscore the complex nature of payment card security and the need for ongoing vigilance. A complex problem cannot be solved by any single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society—business, standards-setting bodies, policymakers, and law enforcement—must work together to protect the financial and privacy interests of consumers. Today as this committee addresses the issue of data breaches, we know that there are criminals intent on inventing the next threat.

There is no time to waste. The PCI Security Standards Council and business must commit to promoting stronger security protections and continuous effort of their effective use while Congress leads efforts to combat global cyber-crimes that threaten us all.

We thank the Committee for taking an important leadership role in seeking solutions to one of the largest security concerns of our time. Our conversation should not end today. We embrace the opportunity to work with you to develop the most practical and feasible solution to addressing cyber and data security threats.

###

Written Testimony of

**Jason Oxman, CEO
The Electronic Transactions Association**

**House Financial Services Committee
Hearing on
“Protecting Consumers: Financial Data Security in the Age of Computer
Hackers”**

May 14, 2015

Introduction:

Chairman Hensarling, Ranking Member Waters, and members of the Committee, I am Jason Oxman, CEO of the Electronic Transactions Association (ETA), and I submit this written statement for the record for the hearing on Protecting Consumers: Financial Data Security in the Age of Computer Hackers. By way of background, ETA is a global trade association whose mission is to advance the payments technology industry. As the trade association of the payments industry, the ETA represents more than 500 of the world’s most innovative payments and technology companies, from Fortune 500 financial institutions, to small, local sales organizations, to the world’s largest technology companies. ETA’s members are dedicated to providing merchants and consumers in our country the safest, most reliable, most secure payments system to facilitate commerce and power our economy. At the outset, I want to affirm ETA’s strong support for legislation that creates uniform, national data breach and data protection standards that are industry neutral, preemptive of state law, such as H.R.

2205 does, and we applaud Chairman Neugebauer and Rep. Carney, as well as the entire Committee leadership, in this regard.

The Electronic Payments Ecosystem – Driver of Economic Growth:

To help put the electronic payments industry into context, when a consumer buys something from a merchant, they often will use a form of electronic payment, such as a credit card, debit card, gift card, prepaid card. Purchases can be made in person with the card or with a mobile device, or remotely, over the phone or the Internet. While the transaction is simply and securely completed within seconds of a swipe or tap, it involves an enormous and complex electronic payments ecosystem, which includes:

- consumer card issuing banks;
- the card brand networks that connect merchants and consumers;
- payment processors that connect merchants with networks of banks (issuing and acquiring) to ensure the transaction is authorized and processed;
- program managers that work with consumers and issuing banks to help consumers obtain credit and prepaid cards;
- point of sale equipment hardware and software companies;
- program managers that work with consumers and issuing banks to help consumers obtain credit and prepaid cards;
- enablers of payment technology and e-commerce;
- merchant acquirers, which provide payment acceptance services;

- independent sales organizations that work directly with merchants to provide access to the payments system;
- sponsor banks, which establish policies for merchant acquirers, sponsor their registration with the card brands, and hold the risk of payment;
- anti-fraud companies that work with providers in the ecosystem to help ensure fraudulent transactions do not occur; and
- security companies that work with all other providers in the ecosystem to protect and secure transactions against intrusion.

This ecosystem is largely invisible to consumers and merchants because it works seamlessly to process billions of transactions each year – that’s literally thousands of transactions every second. Electronic payments are key drivers of commerce and economic growth in our country. To put this into greater context: 70% of U.S. GDP is attributed to consumer spending, and 70% of consumer spending is done electronically. Last year, electronic payments surpassed \$5 trillion and electronic consumer spending will only continue to grow. Indeed, by 2017, we project that ETA member companies will process \$7.3 trillion in consumer spending in the U.S.

Lessons Learned from 2014: The Year of the Breach

You have asked me to address why and how data breaches occur. Some have dubbed 2014 as “The Year of the Breach,” and this past year businesses of all sizes, across various industries, those who store, transmit or process payment card data and

those that contain other valuable information, experienced a breach. By and large, the types of high-profile breaches we saw last year were caused by cyberattacks perpetrated by highly-sophisticated, international criminals, and we should not forget that those businesses who were attacked are, like consumers, also the victims of a crime. Moreover, according to Trustwave, an ETA member company, there are a number of important lessons learned based on information collected from hundreds of post-breach forensic investigations:

1. Misconfiguration issues persist, including the use of weak passwords such as "Password1" and using the same password for multiple logins.
2. Lack of resources limits the time or manpower necessary to make sure that adequate security technology is installed, updated, monitored and continuously working properly.
3. There are security weaknesses across third party providers. The industry has taken steps to require third party providers to use a unique password for each client and two factor authentication.
4. Lack of segmentation, whereby businesses mix all of their networks together so that all of their data – sensitive and non-sensitive – flows through the same networks.

The Electronic Payments Industry's Commitment to Securing Customer's Information:

ETA member companies take seriously their affirmative and continuing obligation to protect the confidentiality and security of their customers' information. Our payments systems are built to detect and prevent fraud -- and to insulate

consumers from any liability. In fact, consumers in the United States choose electronic payments over cash and checks in large part because they have zero liability for fraud, making electronic payments the safest and most reliable way to pay. The liability is borne by companies in the payments industry due to Federal law and even more stringent payment network rules. In light of this financial responsibility and a desire to preserve consumer confidence in the security of electronic transactions, ETA members have a strong interest in making sure fraud does not occur, including through the misuse by criminals of consumer data that happens to be compromised through a data breach. Towards that end, payments technology businesses are bolstered by robust compliance practices – whether their own in-house policies, or ETA’s own carefully crafted industry *Guidelines*, which establish underwriting practices to help payments companies detect and eliminate fraud.

Importantly, for those companies that follow them, self-regulatory guidelines help ensure that consumer data is secure. The Payment Card Industry Data Security Standard (PCI-DSS) created by the PCI Security Standards Council, is an example of one such successful industry-led, multi-stakeholder program, safeguarding personal information that should serve as a model. As a point of reference, fraud accounts for less than six cents of every one hundred dollars spent on the payments systems – a fraction of a tenth of a percent – and the payments industry is on the cutting edge of technology to help further limit fraud. But inasmuch as we just emerged from 2014, which the media dubbed “the year of the data breach” following several high profile

breaches, I would like to highlight five concrete steps the payments industry is currently taking to further combat data breaches and protect consumer information against increasingly sophisticated cyber criminals:

(1) ETA Members: Embracing the EMV migration

ETA has long championed adoption of EMV enabled chip cards as one protection for consumers. EMV enabled chip cards, which can be identified by a conspicuous chip on the card's face, currently only make up about 1%-5% of total card circulation in the US, but this number is expected to increase to 90-95% within the next two years.

To incentivize more rapid migration to EMV adoption, the payments industry faces an October 2015 liability shift for their card transactions, at which point any participant in the transaction chain who is not EMV compliant will be responsible for any resulting fraud. This industry-led initiative is an example of how payments companies are proactively working to strengthen protection for consumers and the payments system.

To explain further, EMV, which stands for EuroPay, Mastercard, Visa, is the global standard for integrated circuit, or "chip" cards. Today, EMVCo (the body that sets that EMV standard) is owned jointly by American Express, Discover, JCB, MasterCard, UnionPay, and Visa, and includes other organizations from the payments industry. EMV cards feature embedded microprocessor chips that store and protect cardholder data – similar to magstripe, but safer. An EMV card is superior to a traditional magstripe card because it supports dynamic authentication. EMV technology does this by encrypting

account information and generating a unique, or “dynamic,” one-time security code for each transaction, which makes the card nearly impossible to replicate. Counterfeiting such cards is currently far more difficult than producing cards with data that is “skimmed” from the magnetic stripes of genuine cards or stolen from stored payments data, such as the high-profile merchant breaches of recent months. Because EMV cards generate a dynamic security code with each transaction, unlike a magnetic stripe card which uses the same static code with every purchase, a counterfeit card could not successfully produce the correct security code and would not work in a card-present or face-to-face transaction. Accordingly, EMV is an effective tool to combat the manufacture and use of counterfeit cards and card-present fraud. But although chip cards reduce the value of compromised data by inhibiting the creation of counterfeit cards, they do not stop data breaches. Other initiatives within the industry further augment the protections provided by EMV and will help erect additional barriers to bad actors, while simultaneously reducing the value of the data they may attempt to obtain.

(2) ETA: Chip and Cardholder Verification Methods

A separate question, independent of the EMV migration, has arisen regarding whether consumers should be required to use a personal identification number (PIN) for each credit card transaction at the point of sale. The EMV chip functions as a fraud prevention tool by generating a dynamic security code, thus preventing the production of counterfeit cards, the single largest (by far) cause of fraud. Put another way, this

ensures that the card itself is valid. It is important to note that a PIN is a method of verifying the cardholder's identity (not that the card itself is valid, but rather that, in theory, the person presenting the card is the actual cardholder). This is referred to as a cardholder verification method, or CVM. A CVM prevents a type of card fraud called "lost and stolen" fraud – where a criminal has stolen a physical card from a wallet, for example, and then attempts to use the card before it has been reported stolen. Other methods of CVM include signature and, in some cases, no CVM is required, for example, because the transaction is a low dollar amount or low risk of fraud, and a CVM would not be beneficial to require.

ETA strongly supports the migration to EMV, and we believe that card issuers should be permitted to make the choice that is best for their customers as to cardholder verification method to accompany the chip cards, whether it be signature, PIN, or neither, when authorizing a transaction. Consumers and merchants have benefitted from flexibility in cardholder verification methods – including speedier checkout times for low dollar, low risk transactions. For example, drive throughs, quick service restaurants and convenience stores, in collaboration with payments companies and card networks, allow consumers to move quickly through checkout lines through "swipe and go" transactions that benefit all parties to the transaction and help maintain overall consumer satisfaction. Similarly, new mobile payments technology replaces traditional CVMs with even more secure biometrics that promise both fraud protection and consumer convenience at a higher level. An important part of the decision of card

issuers whether to require their customers to use a PIN is whether merchants have the capability to accept PIN as a CVM. It should be noted that, at present, roughly 2/3 of the nation's merchants do not have a PIN pad and thus cannot accept a PIN transaction from their customers. For such merchants, consumers who are required to use a PIN for a transaction could represent lost customers.

Similarly, mobile payments cannot use a static PIN with the transaction. As merchants and consumers move from plastic cards to mobile devices, including mobile phones and wearables, this next generation of payments technology must not be inhibited by plastic card-era systems. Also, many consumers prefer not to have to remember PINs. Indeed, in 1967, the inventor of the ATM, John Shepherd-Barron, first envisioned a six-digit numeric code for customer authentication, but his spouse could only remember four digits, which became the commonly used length. Furthermore, the PIN is static and can be stored on a card, making it vulnerable to interception or even being guessed (there are only 10,000 possible 4 digit PIN combinations). As our industry moves to dynamic security, biometrics, and other systems that are even more secure, we must consider these important factors in making the right choice to secure transactions.

The fact remains that criminals are adaptive and constantly probe for vulnerabilities. Focusing on one specific technology gives hackers an open invitation to focus their energies on that technology and to detect and exploit loopholes in the payments system. Strong security involves a multi-layer approach which has the ability

to evolve in response to the changing threat environment, allowing the industry to be as nimble as the bad actors it is attempting to thwart. At the end of the day, we all need to work continuously and collaboratively across banks, payments companies, merchants and consumers to find the most effective and efficient security mechanisms.

(3) ETA Members: Fostering other new technology

As previously mentioned, EMV is one part of the overall, multi-layered solution to protecting data, consumers, and the payments system. ETA members are simultaneously deploying new innovations to further enhance security. For example, another technology, tokenization, removes sensitive information from a transaction by replacing customer data with a unique identifier that cannot be mathematically reversed. In its simplest form, it works like a secret code substituting symbols for important information like a credit card number. This way, only banks and payment processors know real account information. Tokenization is designed to work when a consumer pays with plastic in person, online or with a mobile phone.

In a non-tokenized transaction, a consumer's actual account number is transmitted and, in some cases, stored by retailers, e.g., for purposes of facilitating returns. This trove of information is what hackers typically seek in the case of retailer data breaches. But in a tokenized environment, actual account numbers are replaced by one time-use tokens that represent account numbers but cannot be tied back to the actual number. If a breach occurs, the criminal only sees the tokenized code, which is

useless to them because it cannot be used to generate a subsequent fraudulent transaction.

Another layer of protection deployed by ETA member companies is the use of point-to-point encryption. Point-to-point encryption is an advanced risk management tool that helps further protect data throughout the transaction lifecycle. With point-to-point encryption, card data is encrypted from the moment the card is swiped or tapped, while the data is in transit, all the way to authorization. This technology minimizes opportunities for hackers and criminals to access data during a purchase.

Additionally, many payment companies continue to innovate advanced computer systems that monitor transactions and data patterns detect unusual activity that may indicate an account has been hacked or a card lost or stolen. This monitoring occurs in both traditional, card-present as well as in card-not-present transactions, such as those taking place over the Internet or phone. Lastly, using a mobile device to initiate a transaction will soon be as common as swiping a card. Mobile payments and digital wallet cloud technology are actively employing new security technology that improves on legacy systems. Mobile devices provide enhanced security, including passcode protection for the phone, biometrics security features like a fingerprint, secure chip technology, geo-locational information to assist with verification, as well as both device and cloud based encryption and tokenization capabilities.

The payments industry is creating innovative solutions today to solve tomorrow's security threats. This protection ensures the flow of information vital to helping

consumers access and use electronic payments, promotes competition and ensures the free flow of commerce, and maintains public confidence. It is imperative to find ways to encourage new technologies and enterprises, ensuring that the payments revolution will realize its maximum potential.

(4) ETA Members: Supporting Legislation to Promote Information Sharing

In addition to self-regulation and new security technology, ETA is working to remove barriers that prevent government and industry from sharing information about cyber threats. One lesson learned from recent high profile data breaches is that they are being perpetrated against U.S. companies by highly sophisticated and global cybercriminals. Along these lines, ETA is strongly supporting legislation, such as H.R. 1731, the "National Cybersecurity Protection Advancement Act of 2015"¹ and H.R. 1560, the "Protecting Cyber Networks Act," both of which would promote sharing of Internet traffic information between the U.S. government and technology and manufacturing companies in order to help the government investigate cyber threats and ensure the security of networks against cyberattacks. Such legislation would provide a simple and effective means of sharing important cyber threat information with the government.¹

(5) ETA Members: Supporting Legislation to Stream-line Consumer Notification of Breaches and Data Protection

Perhaps most pertinent to this hearing today, this Committee and the U.S. Congress have an important role to play in protecting consumers in the United States from the criminals who prey upon the financial system. One area ripe for reform is the

¹ HR 1731 has been merged into HR 1560.

unworkable and harmful state of regulations regarding consumer notification of breach events.

Currently, there is a patchwork of 47 separate state data breach notification laws with which retailers and the payments industry must comply, making uniform notifications virtually impossible while simultaneously making the process of notifying customers more costly, more cumbersome, and less timely. ETA is strongly supporting legislation to create, as H.R. 2205 does, a uniform national standard, preemptive of state law, for reporting financial data security breaches. One standard will provide certainty and predictability to consumers and the industry.

On setting a uniform data protection standard, ETA strongly supports the provisions in H.R. 2205, the *Data Security Act of 2015*, making data security a federal requirement for non-banks. The provision in the bill is both technology- and industry-neutral and flexible, reflecting the rapidly changing pace of technology and the wide array of companies that serve a major role in the current payments ecosystem. Protection of consumer data is crucial for all participants in the payments space to help prevent cyber theft of consumers' information. H.R. 2205 recognizes this, and ETA supports the bill.

Conclusion:

Headline-grabbing events inevitably lead to calls for additional government regulations. The members of the ETA are the first line of defense for consumers to avoid the fraud perpetuated by criminals in the financial systems. As described, the

payments industry takes seriously this charge and works hard every day to detect and deter crime. ETA members are deploying multiple layers of protection, including EMV, tokenization, encryption, biometrics, and other payments technologies that secure systems against criminal intrusions and protect consumers and merchants. While we support legislation to provide a uniform, federal breach notification law, and flexible data protection standards for the payments industry, we believe that new burdensome regulations that dictate payment technology would ultimately harm consumers and retailers and would stifle nascent marketplace innovations that hold great promise for reducing future criminal activities and enhancing the payments system. Indeed, such regulation could be counterproductive, making the industry less capable of responding to the adaptive methodologies of cyber criminals and constraining the industry within a narrow band of allowable technologies on which criminals could concentrate their attacks.

As the trade association of the payments industry, ETA stands ready to assist the Committee in its efforts to ensure that consumers, merchants, and the economy continue to benefit from the safety and security of our nation's payments systems.

² Currently, the U.S. Secret Service, the US Computer Emergency Readiness Team, and the US Department of Homeland Security participate in information sharing through VERIS (Vocabulary for Event Recording and Incident Sharing), but more is needed.

110

May 14, 2015

Testimony of
Tim Pawlenty

On behalf of

The Financial Services Roundtable

Before the

**United States House of Representatives
Committee on Financial Services**

Hearing on

“Protecting Consumers: Financial Data Security in the Age of Computer Hackers”

Chairman Hensarling, Ranking Member Waters and Members of the Committee, thank you for having me here today.

On behalf of the members of the Financial Services Roundtable,¹ I appreciate the opportunity to discuss the challenges consumers and businesses face from data breaches and the growing need to enhance data security efforts. The entire financial services industry – from the diverse members of FSR to the approximately 14,000 community banks and credit unions in this country – are united on efforts to protect consumers and prevent the type and volume of incidents that led 2014 to be dubbed “the year of the breach.”²

My testimony today will cover the following topics:

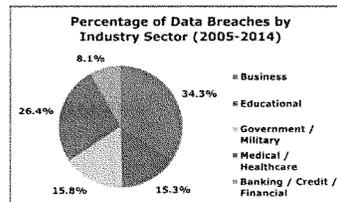
- A macro overview of data breach trends;
- How the payments system is evolving, and the importance of forward-looking security and technology;
- The clear need for Congress to enact “bank-like” data security requirements for all industries and common-sense consumer breach notification standards; and
- How current legislation, the Data Security Act of 2015 (H.R. 2205), accomplishes these goals by providing the highest level of consumer protection found in any bill currently introduced in the House.

Data Breaches: An Ongoing Challenge

No entity is immune to hackers. There's a common saying that there are two types of businesses: those who know they've been hacked, and those that have been hacked and just don't know it yet.

Not surprisingly, financial institutions are a common target. As the data in Figure 1 show,

Figure 1



Source: Identity Theft Resource Center

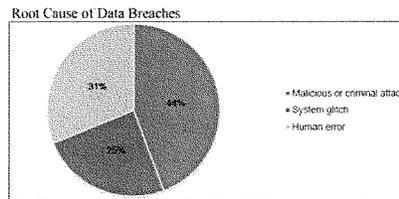
¹ The Financial Services Roundtable represents the largest integrated financial services companies providing banking, insurance, payment and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America's economic engine, accounting for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs.

² <http://www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach/>

however, they seem to do better than any other major sector at defeating most of those attacks. Financial institutions accounted for only 8.1%³ of data breaches in the U.S. between 2005 and 2014. Such results can be attributed, in part, to how the industry has adjusted to the changing cyber landscape. For example, the collaborative, real-time threat information sharing facilitated through the Financial Services – Information Sharing and Analysis Center (FS-ISAC) – a public-private partnership between financial services providers, commercial security firms, law enforcement and all levels of government – allows the industry to maintain the highest levels of threat preparedness and rapid response capabilities in the private sector.

Figure 2

As Figure 2 shows, data breaches occur for many reasons and in many ways.⁴ “Phishing scams” are one common method hackers employ to gain access to systems. Such scams were a common entry point in several high-profile data breaches at retailers last year. Those scams allowed access to one portion of retailers’ network infrastructure and that access eventually allowed the criminals to inject malware into point-of-sale systems to skim payment card data.⁵



Hacking methods aren’t always that sophisticated, however. A simple unlocked door granting unauthorized access to a server, or a misplaced USB drive containing a spreadsheet of customers’ sensitive information are also recent examples of how systems were breached and sensitive information was exposed. Many data breach incidents are preventable if proper safeguards and controls are in place.

Data breaches of sensitive financial information are, of course, costly for all parties involved. For example, financial institutions often bear much of the costs after a breach involving debit or credit cards, including the cost of card reissuance, covering fraudulent charges to uphold “zero liability” protections for customers, and reputational damage that is associated with a breach. The breach that occurred at Home Depot last year is estimated to have cost the credit union and community banking industries alone \$60 million⁶ and \$90 million⁷ respectively. A single large issuer may spend over \$10-\$20

³ <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html>

⁴ “2014 Cost of Data Breach Study: United States,” Ponemon Institute. May 2014.

⁵ <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/>

⁶ http://news.cuna.org/articles/53M_email_addresses_stolen_in_HD_breach_impact_on_CUs_mounts

⁷ <http://www.icba.org/news/newsreleasedetail.cfm?ItemNumber=189537>

million to reissue a portfolio of millions of card to mitigate just one major retail data breach.

The Fast-Evolving Payments System

Payment technology is rapidly evolving, and the financial services industry is driving much of the investment and innovation that will shape the future payments system.

In the near-term, cards will be much more difficult to counterfeit through the use of computer chips embedded in the cards as well as “tokenization” technology to make stolen data virtually worthless to criminals. In the future, new methods of identity verification that not long ago were the stuff of Hollywood movies – voice, facial recognition, biometric, location verification, gesture and behavior-based authentication, and more – will likely reduce or eliminate the need for traditional PINs and passwords.

Mobile payments, while still a small percentage of overall transaction volume, have gained great momentum in the marketplace and they will soon represent a significant portion of payment volume. Innovation and investment in payment security will increase as consumer adoption of mobile payment systems increases.

As policymakers consider a legislative response to data breaches, it is important to remember that no single card technology will prevent all data breaches. Effective defense strategies will require prevention across the entire interconnected payments system, not just one area or element of that system. Industries need to be holistic in their approach and parties to a payment transaction should layer security technologies to keep customers as safe as possible.

U.S. Migration to EMV

Later this year, a significant portion of the payments industry will undergo a fundamental change. Card networks have announced that starting in October, card issuers and merchants that implement certain stronger security technology will not be liable in the case of fraud, while companies that do not implement such advanced technology could be liable for fraud.

The technology driving this liability shift is EMV -- an acronym for Europay, MasterCard, Visa – which is a technical standard that enables chip cards to effectuate a more secure transaction. EMV chip cards are effective at preventing card counterfeiting, which helps reduce the amount of card-present fraud following a data breach of payment card

account numbers or other sensitive information.⁸ However, EMV does not help prevent online fraud where a card is not physically used.

Many other countries have already moved to wide-scale EMV card acceptance. The reasons why the U.S. is just now making the shift to EMV chip card technology are worth reviewing.

The U.S. card market is somewhat unique in ways that make the shift to EMV more challenging. For example, most other EMV markets do not have 14,000 financial institutions and tens of millions of merchants that need to move in relative unison to implement EMV. Furthermore, the total volume of non-cash transactions in the U.S. is double that of the *entire* Eurozone.⁹ So, the magnitude of the change is different in the U.S. and that change requires a significant overhaul of current systems. In considering those needed changes an industry representative stated the migration to EMV "...is comparable to declaring that U.S. drivers will now drive on the left-hand side of the road and changing all the road signs and highway entrance and exit ramps and reprogramming all the GPS systems."¹⁰

In any event, the changeover to EMV is now being implemented in the U.S. and its benefits will soon be available to American consumers and businesses.

Thinking Pragmatically about PINs

As policymakers contemplate federal policy regarding the future of payment security and related consumer protection, numerous factors should be considered. One such factor is recognizing government is not well-suited to predict or pick optimal future technology. Payment technology is changing and improving very rapidly. A government embrace of any one particular technology or approach is likely to limit more and better options as new technologies in this space now seem to emerge nearly each week.

- 50-year-old technology should not define the future of payment security:
Magnetic stripe technology was invented in the 1960s and it revolutionized the payments system at the time. PIN technology was also invented in the 1960s.¹¹ Both magnetic stripe and PIN technologies are dated and they are understandably being passed by more forward-leaning payments security technology.

⁸ <http://usa.visa.com/personal/security/chip-technology/emv-chip.jsp>

⁹ Capgemini *World Payments Report 2013*.

¹⁰ <http://arstechnica.com/business/2014/08/02/chip-based-credit-cards-are-a-decade-old-why-doesnt-the-us-rely-on-them-yet/>

¹¹ See <http://news.bbc.co.uk/2/hi/business/6230194.stm>

In addition, it is important to remember that most merchants do not even currently accept PINs. According to the Federal Reserve, only 25% of merchants accepting debit cards accept PIN-based debit transactions.¹² According to point-of-sale (POS) hardware manufacturer Ingenico, of the nearly 3 million POS terminals at large merchants, nearly all have PIN capability. On the other hand, virtually none of the 22 million “micro merchants” have the current capability to accept PINs. Obviously, there is a big gulf between large and small merchants in their ability to accept PINs.

- Banks and retailers are moving to more secure forms of authentication beyond PIN: Payments innovators are abandoning static data elements in favor of dynamic, single-use technologies that can render stolen data useless to criminals. Financial institutions are also continuing to develop new ways to authenticate customers that don't rely on just one factor, like a password or a PIN. Biometric authentication is becoming an integral part of mobile payments, and other technologies focused on multiple factors, including gesture or behavior-based authentication, are being considered to help secure access to sensitive systems and transactions. BITS, the technology policy division of FSR, is collaborating with its members in the High Assurance Authentication Project which will help define optimal financial services technologies and practices for stronger authentication techniques.

As consumers, most of us have probably noticed that more and more transactions don't even require a signature, let alone a PIN. According to data from Visa, more than 60% of Visa's U.S. transaction volume qualifies for no customer verification method at all because they are low-dollar and low-risk.

- No “silver bullet” has yet been developed to fully stop payment breaches and related fraud: In countries where EMV chip cards are utilized throughout their payments system, fraud rates from lost, stolen or counterfeit use at the point-of-sale have declined. However, after the introduction of EMV cards, in many instances overall fraud rates increased significantly due mainly to very large increases in card-not-present (CNP) fraud (i.e., online shopping).¹³ Technologies are being developed to better address fraud in CNP situations.

¹² Federal Reserve Board of Governors. *Regulation II, Final Rule*.

¹³ See Appendix 1.

Looking Forward in Payment Security

More innovation is taking place in payments than arguably in any other aspect of financial services. From increasing security and reducing fraud to creating a more friction-free experience for consumers, the financial services industry is committed to maintaining its role as consumers' trusted source for payments and managing money. With the support and drive from the financial industry, biometrics, cloud-based technology, location-based services, and keystroke behavior patterns will be the norm in the future. More immediately, the development of tokenization-- the process of replacing sensitive financial information with data that can only be interpreted by a very limited set of parties in the transaction chain-- is paving the way for mobile payments to become viable.

Transactions using tokenization help ensure stolen data is of no value in a data breach. Tokenization, along with biometrics or other layered security measures, help create a more secure mobile payment experience. Again, there is no single panacea to preventing fraud and stopping data breaches.

Creating "Bank-Like" Security for Firms of All Sizes

Congress should pass legislation creating a strong, meaningful data security requirement for all companies that handle sensitive customer information but currently have no federal requirement to protect it.

The Gramm-Leach-Bliley Act (GLBA) (Pub.L. 106-102), enacted in 1999, directed the Federal Trade Commission and federal and state regulators with oversight of financial institutions to establish appropriate standards and processes relating to administrative, technical and physical safeguards to protect customer information.

For the financial industry, the GLBA is implemented and enforced by pertinent federal and state regulators. For example, the federal banking agencies establish information security standards for banks and regularly examine banks for compliance with those standards, while the Securities and Exchange Commission oversees broker-dealers and investment advisors and state insurance departments oversee insurance companies in this regard.

The GLBA's standards and processes apply to the smallest credit union or community bank as well as the largest financial firms in America. This is made possible by the flexibility built into the GLBA standards that allow adjustments for the size and complexity

of the financial institution, the nature and scope of its activities, and the sensitivity of the information it handles.¹⁴

Addressing Small Business Concerns

While a clear need exists for Congress to enact strong data security legislation, any standard or process Congress creates should not be prescriptive, inflexible or overly burdensome for small businesses. For the reasons outlined above, a flexible standard that is adaptable to both the size of the entity and the changing nature of data security technology is the most common-sense approach. Such a standard has served the financial service sector and its customers well.

Similar to small financial institutions, small businesses frequently rely on third party vendors to implement and maintain core business functions like payment processing and data security.¹⁵ In addition to providing the service, compliance responsibilities would likely be delineated via contract with such vendors.

Most small and medium-sized businesses do not maintain data centers or other extraordinary in-house technology that would be likely to invite significant new compliance requirements were Congress to enact bank-like security process requirements. However, it is highly likely that third-party service providers, particularly payment providers, will pay closer attention to the controls even the smallest of businesses has in place to protect customer information.

For example, it is not unreasonable to expect any size business to password-protect systems with something more robust than "password" or "123456." If a small business has a server or PC on which it maintains customer files with sensitive financial information, it would be wise to implement physical safeguards, such as a lock on the door with limited access. If a small business has a wireless internet network, it should be required to have at least minimal security features.¹⁶

This list is not exhaustive but is illustrative of the basic nature of data security requirements that can help prevent breaches yet are too often absent today.

¹⁴ See *Interagency Guidelines Establishing Information Security Standards*. Accessed at <http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm>

¹⁵ See, for example: National Small Business Association, "2013 Small Business Technology Survey," accessed at <http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf>

¹⁶ For example, the 2007 breach at nationwide retailer TJ Maxx was caused by an unsecured wireless network that allowed hackers clear access to payment card information. See <http://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/>

The Right Legislation is Needed

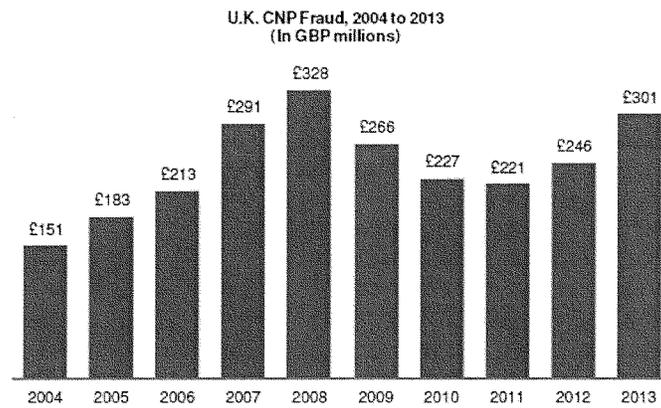
Enacting the right data breach legislation will create a framework of complementary federal requirements and self-regulatory standards, such as those put forth by the PCI Security Standards Council. FSR, and many others in the financial industry,¹⁷ believe data security and notification legislation should include the following elements:

- A data security requirement establishing the framework for a flexible, scalable process firms should follow to implement administrative, technical and physical safeguards to ensure the security, confidentiality and integrity of sensitive consumer financial information.
- A common-sense notification process firms should follow in the event they discover a breach of information that could put consumers at risk of harm, and that ensures consumers are notified in a timely manner, but that allows for a reasonable delay for law enforcement investigation.
- Preemption of the patchwork of conflicting state data breach laws for all industries.
- A recognition that certain industries – like healthcare and financial services – already comply with federal data security and consumer notification standards, to ensure those industries are not faced with duplicative, unnecessary regulatory requirements.

Such provisions are contained in H.R. 2205, the Data Security Act of 2015, introduced by Congressman Randy Neugebauer and Congressman John Carney. *No other bill introduced in the House this session approaches the level of consumer protections contained in this measure.* Its provisions are reasonable, not overly burdensome on businesses, and will help stop the flow of data breaches. We encourage Members of this Committee to support this important measure along its path toward enactment.

Thank you for inviting me to testify. I look forward to your questions.

¹⁷ For more information, see joint letter from FSR, ABA, CBA, The Clearing House, NAFCU, CUNA and ICBA: <http://fsroundtable.org/fi-trades-sends-joint-letter-house/>

Appendix 1

Source: Julie Conroy. "EMV: Lessons Learned and the U.S. Outlook," Aite Group. June 2014

The U.K. payments ecosystem began a transition to EMV chip technology in 2001. In 2005, a liability shift occurred in which the entity with the lowest form of technology (i.e., not EMV-compliant), would be responsible for fraud on a given transaction.

Between the date of the liability shift in 2005, card-not-present fraud increased dramatically, peaking at GBP328 million in 2008, a 79% increase.



Statement for the Record
House Committee on Financial Services

Hearing titled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers"

May 14, 2015

The American Council of Life Insurers (ACLI) is pleased to submit this statement for the hearing record expressing the views of the life insurance industry regarding the protection of sensitive nonpublic consumer information.

The American Council of Life Insurers (ACLI) is a Washington, D.C.-based trade association with approximately 300 member companies operating in the United States and abroad. ACLI advocates in federal, state, and international forums for public policy that supports the industry marketplace and the 75 million American families that rely on life insurers' products for financial and retirement security. ACLI members offer life insurance, annuities, retirement plans, long-term care and disability income insurance, and reinsurance, representing more than 90 percent of industry assets and premiums.

Life insurers' relationships with their customers are personal and confidential. Life insurers recognize that their customers expect them to maintain the security of their nonpublic personal information and acknowledge their affirmative and continuing obligation to do so.

ACLI supports a uniform national standard for notification to individuals whose personal information has been subject to a security breach. A uniform national standard will ensure that consumers receive clear, consistent notice regardless of where they live or the type of entity subject to the breach and eliminate the complexity and burden of complying with the current patchwork of 48 differing state breach notification laws. Accordingly, ACLI supports federal legislation that provides a uniform national standard for breach notification and expressly preempts any related state breach notification standards.

ACLI member companies also support legislation that avoids needlessly alarming consumers, by requiring notice only when a breach in the security of consumers' nonpublic personal information is likely to cause harm, and by not requiring notice if consumers' nonpublic information is protected by encryption or some other means that makes the information unreadable or unusable.

ACLI applauds Representatives Randy Neugebauer and John Carney for their efforts to craft federal legislation, H.R. 2205, that reflects the fundamentally important principles described above. We appreciate their leadership in support of strong consumer protection. We look forward to working with them and this Committee on issues of importance to the life insurance industry and its policyholders as the bill moves through the legislative process.

Thank you for convening this important hearing and for your consideration of the views of ACLI and its member companies.



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

National Association of Federal Credit Unions | www.nafcu.org

May 13, 2015

The Honorable Jeb Hensarling
Chairman
House Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

The Honorable Maxine Waters
Ranking Member
House Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing, "Protecting Consumers: Financial Data Security in the Age of Computer Hackers"

Dear Chairman Hensarling and Ranking Member Waters:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the interests of our nation's federal credit unions, I write today regarding tomorrow's hearing entitled, "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." A primary concern of credit unions and their 100 million members continues to be data breaches at our nation's retailers exposing financial and personal data of millions of consumers. We thank you for holding this important hearing and applaud your leadership on this matter.

As you know, consumers at risk in the wake of a data breach often rely on their credit union to help re-establish financial safety. In the process, credit unions suffer steep losses through the reissuance of cards, the charge-off of fraud, and the staff time it can take to respond to the magnitude of many of the breaches we have seen recently. Unfortunately, not all entities are held to a federal standard in protecting sensitive financial and personal information. While credit unions have been subject to federal standards on data security since the passage of *Gramm-Leach-Bliley Act* in 1999, the same cannot be said for our nation's retailers.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. 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 and notify consumers when a breach occurs that will put them at risk—no matter what size of the institution. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to \$1 million per day for compliance violations. These extensive requirements and safeguards have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999 as part of the *Gramm-Leach-Bliley Act (GLBA)*. In contrast, retailers are not covered by *any* federal laws or regulations that require them to protect the data and notify consumers when it is breached.

The ramifications for credit unions and their members have been monumental. A February of 2015 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were \$226,000 on average. Of their losses, respondents expect to recoup less than 0.5%, which amounts to less than \$100 on average. Despite the claims of some trade groups, the fact remains that our members are not recovering anything close to what they are spending to make their members whole after a merchant breach.

NAFCU believes legislation pending before the committee, H.R. 2205, the *Data Security Act of 2015* would help address these concerns. This legislation would create a national standard of data security for all industries that handle sensitive information based on the standards in *Gramm-Leach-Bliley Act* (GLBA), a key priority of NAFCU. We are also pleased that it would recognize that it is not productive to duplicate data protection and consumer notice requirements that are already in place for credit unions under GLBA. We urge the committee to support this legislation and move it to mark-up as soon as possible.

Thank you for your attention to this important matter. We look forward to tomorrow's hearing and working with the committee as you move forward in addressing data security issues. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Director of Legislative Affairs Jillian Pevo at (703) 842-2836.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the House Financial Services Committee



May 14, 2015

Chairman Jeb Hensarling
U.S. House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Ranking Member Maxine Waters
U.S. House of Representatives
Committee on Financial Services
4340 O'Neill Federal Office Building
Washington, DC 20515

Re: Insurance Consumer Data Protection

Dear Chairman Hensarling and Ranking Member Waters:

On behalf of the National Association of Insurance Commissioners (NAIC)¹, we write today to thank you for holding a hearing on "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." State insurance regulators take very seriously our responsibility to ensure the entities we regulate are protecting the many kinds of highly sensitive consumer information they retain. In this regard, we are acutely aware of the complex mission insurance regulators have of protecting consumers, laying out expectations for the insurance industry, and recognizing the economy-wide role insurers can play in driving best practices and mitigating the financial aftermath of a cyber attack.

As you know, insurance companies in the United States are subject to a stringent state-based regulatory regime designed with the primary mission of protecting policyholders. Consumer data privacy and cybersecurity issues are not new to state insurance regulators – the NAIC's *Standards for Safeguarding Consumer Information Model Regulation* sets forth standards that insurance entities must meet to be in compliance with federal and state information security laws and regulations, and the NAIC examiner handbooks for financial and market conduct exams include extensive guidance on examining controls to confirm insurance entities are taking necessary steps to protect consumers. Even when an insurer is diligent to secure infrastructure, they may be the victim of a criminal data breach. In such an event, companies are required to inform insurance regulators in all affected states, at which point we work with law enforcement agencies and the affected company to ensure consumers are notified promptly and steps are taken to mitigate potential harm.

¹ Founded in 1871, the NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and the five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S.

EXECUTIVE OFFICE • 444 North Capitol Street, NE, Suite 700 • Washington, DC 20002-1509	p 202-471-1999	f 202-462-5403
CENTRAL OFFICE • 150 Walnut Street, Suite 1500 • Kansas City, MO 64104-7197	p 816-242-2669	f 816-242-2125
CAPITAL MARKETS & INVESTMENT ANALYSIS OFFICE • One One York Plaza, Suite 4210 • New York, NY 10004	p 212-298-9003	f 212-292-4707

www.naic.org

Last November, following numerous discussions about cybersecurity among our members and leadership, the NAIC established a Cybersecurity (EX) Task Force.² After announcing its membership³ this February, the Task Force laid out an ambitious work plan, and while much work remains, we have already made significant progress in our efforts to enhance cybersecurity protections in insurance. Following extensive written and verbal comments by interested parties, on April 16, 2015 the Task Force approved a finalized list of 12 insurance regulatory guiding principles.⁴ We believe these principles create a broad framework to lay out our duties and obligations as regulators and the expectations we have for our sector. The principles will promote accountability across the entire insurance sector in the best interests of consumers. They will serve as the foundation for protection of sensitive consumer information held by insurers and producers while guiding the regulators who oversee the insurance industry.

The Task Force also worked with the NAIC's Property and Casualty (C) Committee to draft a Cybersecurity Insurance Coverage Supplement proposal for the annual financial statement required of insurers.⁵ This filing will provide regulators with more specific information regarding the size of the growing cyber liability market on a nationwide basis. The draft proposal was exposed for comment in March, and is currently under review by several NAIC committees. Additionally, the Task Force is working closely with the Information Technology Examination (E) Working Group to update examination protocols for financial examiners to ensure that cyber security is embedded in on-site examinations of insurers. Similar updated protocols for market conduct examiners are also under consideration.

Additional Task Force plans for the immediate future include a survey of states to assess cyber vulnerabilities, development of a "Consumer Bill of Rights" for insurance data breach victims, webinars on the benefits of information sharing, and a comprehensive review of existing cybersecurity related model laws and regulations.

Consumers have a right to expect that personal financial and health information entrusted to insurers and health care providers is secure. As Congress contemplates legislation in this arena, we encourage you not to limit state regulators' tools or authorities to protect policyholders. While we understand and appreciate the potential benefits of establishing common definitions and cross-sector minimum standards for data security, we remain skeptical of any efforts that involve preemption of a state's right to enact protections for its insurance consumers that go above and beyond those recommended or required by Federal law. We also are concerned with efforts to limit individual state regulators from protecting consumers in their state, regardless of where a breached insurer is domiciled. While well intentioned, such standards may actually undermine existing consumer protections, as well as inhibit future enhancements and innovation necessary for regulators and companies to adapt to evolving threats.

The American public relies on insurance for financial peace of mind, and state insurance regulators are committed to continuing our leadership in this area to maintain the trust of policyholders across the country. We commend your Committee for its attention to the critical issue of consumer data protection, and look forward to working with you to design a strong data protection framework that is in the best interests of insurance consumers.

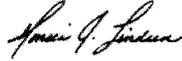
² Attachment A – NAIC Press Release, November 19, 2014.

³ Attachment B – Cybersecurity (EX) Task Force Membership List

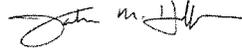
⁴ Attachment C – Adopted Principles for Effective Cybersecurity: Insurance Regulatory Guidance

⁵ Attachment D – Proposed Cybersecurity Insurance Coverage Supplement

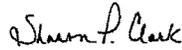
Sincerely,



Monica J. Lindeen
NAIC President
Montana Commissioner of
Securities and Insurance



John M. Huff
NAIC President-Elect
Director of Missouri's Department of Insurance,
Financial Institutions, and Professional Registration



Sharon P. Clark
NAIC Vice President
Kentucky Insurance Commissioner



Theodore K. Nickel
NAIC Secretary-Treasurer
Wisconsin Insurance Commissioner



E. Benjamin Nelson
NAIC Chief Executive Officer



FOR IMMEDIATE RELEASE

INSURANCE REGULATORS ESTABLISH CYBERSECURITY TASK FORCE

NAIC forms committee to address emerging issues related to cyber threats

WASHINGTON, D.C. (Nov. 19, 2014) -Today the National Association of Insurance Commissioners (NAIC) formed a special task force to help coordinate insurance issues related to cybersecurity. The task force will make recommendations and coordinate NAIC efforts regarding: the protection of information housed in insurance departments and the NAIC; the protection of consumer information collected by insurers; and collecting information on cyber-liability policies being issued in the marketplace. The group will report and make recommendations to the Executive Committee.

"The threat of a cyber-attack is very real, and state regulators are committed to developing the tools we need to ensure effective regulation in this area," said Adam Hamm, NAIC President and North Dakota Insurance Commissioner. "The American public relies on insurance for financial peace of mind, and our leadership in this area is critical to maintaining that trust."

The creation of the task force is a reflection of the NAIC's growing commitment to addressing cyber security in the insurance sector. State regulators serve on the Treasury Department's Financial Banking and Information Infrastructure Committee and on the Executive Branch and Independent Agency Regulatory Cybersecurity Forum, where they work with Federal regulators to address cyber threats in the U.S. Earlier this year, the NAIC hosted a forum on regulatory challenges as they relate to cybersecurity.

About the NAIC

The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.



Contacts

Communications
Division
news@naic.org

Scott Holeman
Communications Director

Jeremy Wilkinson
Sr. Electronic
Communications
Manager

Miun Gleeson
Sr. Communications
Specialist

Erin Yang
Media Strategist

Katherine Jones
Communications
Specialist

Visit the **NEWSROOM**
for media resources,
archived releases and
alerts

Join Our E-mail List to
receive the latest news
releases and other
information from the
NAIC Communications
Division.

CYBERSECURITY (EX) TASK FORCE

Adam Hamm, Chair	North Dakota
Raymond G. Farmer, Vice Chair	South Carolina
Jim L. Ridling	Alabama
Lori K. Wing-Heier	Alaska
Germaine L. Marks	Arizona
Dave Jones	California
Katharine L. Wade	Connecticut
Chester McPherson	District of Columbia
Kevin McCarty	Florida
Gordon I. Ito	Hawaii
James Stephens	Illinois
Eric A. Cioppa	Maine
Al Redmer Jr.	Maryland
Mike Rothman	Minnesota
John M. Huff	Missouri
Monica J. Lindeen	Montana
Bruce R. Ramge	Nebraska
Scott J. Kipper	Nevada
Roger A. Sevigny	New Hampshire
Kenneth E. Kobylowski	New Jersey
Benjamin M. Lawsky	New York
Mark O. Rabauliman	Northern Mariana Islands
Mary Taylor	Ohio
John D. Doak	Oklahoma
Teresa D. Miller	Pennsylvania
Joseph Torti III	Rhode Island
David Mattax	Texas
Jaqueline K. Cunningham	Virginia
Mike Kreidler	Washington
Ted Nickel	Wisconsin

NAIC Support Staff: Eric Nordman/Sara Robben/Tony Cotto/Cody Steinwand

Principles for Effective Cybersecurity: Insurance Regulatory Guidance¹

Due to ever-increasing cybersecurity issues, it has become clear that it is vital for state insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to aid in the identification of uniform standards, to promote accountability across the entire insurance sector, and to provide access to essential information. State insurance regulators look to the insurance industry to join forces in identifying risks and offering practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers.

Principle 1: State insurance regulators have a responsibility to ensure that personally identifiable consumer information held by insurers, producers and other regulated entities is protected from cybersecurity risks. Additionally, state insurance regulators should mandate that these entities have systems in place to alert consumers in a timely manner in the event of a cybersecurity breach. State insurance regulators should collaborate with insurers, insurance producers and the federal government to achieve a consistent, coordinated approach.

Principle 2: Confidential and/or personally identifiable consumer information data that is collected, stored and transferred inside or outside of an insurer's, insurance producer's or other regulated entity's network should be appropriately safeguarded.

Principle 3: State insurance regulators have a responsibility to protect information that is collected, stored and transferred inside or outside of an insurance department or at the NAIC. This information includes insurers' or insurance producers' confidential information, as well as personally identifiable consumer information. In the event of a breach, those affected should be alerted in a timely manner.

Principle 4: Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 5: Regulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations.

Principle 6: State insurance regulators should provide appropriate regulatory oversight, which includes, but is not limited to, conducting risk-based financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident response by insurers, insurance producers, other regulated entities and state insurance regulators is an essential component to an effective cybersecurity program.

Principle 8: Insurers, insurance producers, other regulated entities and state insurance regulators should take appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.

¹ These principles have been derived from the Securities Industry and Financial Markets Association's (SIFMA) "Principles for Effective Cybersecurity Regulatory Guidance."

Principle 9: Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

Principle 10: Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer's board of directors or appropriate committee thereof.

Principle 11: It is essential for insurers and insurance producers to use an information-sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

Principle 12: Periodic and timely training, paired with an assessment, for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity issues is essential.

W:\National Meetings\2015\Summer\TF\Cybersecurity\Guiding Principle Documents\Final Guiding Principles 4 16 15.docx

CYBERSECURITY INSURANCE COVERAGE SUPPLEMENT

For The Year Ended December 31, 20__

(To Be Filed by April 1)

NAIC Group Code _____ NAIC Company Code _____

Company Name _____

If the reporting entity writes any cybersecurity coverage, please provide the following:

1. Standalone Policies

Direct Premiums		Direct Losses		Direct Defense and Cost Containment		Number of Policies in Force	
1 Written	2 Earned	3 Paid	4 Incurred	5 Paid	6 Incurred	7 Claims Made	8 Occurrence
\$	\$	\$	\$	\$	\$		

1.1 What is the range of the limits offered for the standalone policy? \$ _____ to \$ _____

2. Commercial Multiple Peril Package Policies:

2.1 Does the reporting entity provide cybersecurity coverage as part of a package policy? Yes[] No[]

2.2 If the answer to 2.1 is yes, please provide the following:

Direct Losses		Direct Defense and Cost Containment		Number of Policies with cybersecurity coverage in Force	
1 Paid	2 Paid + Change in Case Reserves	3 Paid	4 Paid + Change in Case Reserves	5 Claims Made	6 Occurrence
\$	\$	\$	\$		

2.3 Can the direct premium earned for the cybersecurity coverage provided as part of a package policy be quantified or estimated? Yes[] No[]

2.4 If the answer to question 2.3 is yes, provide the quantified or estimated direct premium earned amount for cybersecurity coverage included in package policies

2.41 Amount quantified: \$ _____

2.42 Amount estimated using reasonable assumptions: \$ _____

2.5 What is the range of limits offered for the cybersecurity policies? \$ _____ to \$ _____

3. If the cybersecurity policy is a Claims Made policy, is tail coverage offered? Yes[] No[]

3.1 If tail coverage is offered, what is the range of the limits offered? \$ _____ to \$ _____

CYBERSECURITY INSURANCE COVERAGE SUPPLEMENT

This supplement should be completed by those reporting entities that provide cybersecurity coverage in a standalone policy or as part of a commercial multiple peril package policy. The supplement should be reported on a direct basis (before assumed and ceded reinsurance).

Cybersecurity

Coverage for damages arising out of unauthorized use of, or unauthorized access to, electronic data or software within your network or business.

- Line 1 Direct premiums, losses and defense and cost containment expenses for standalone policies are to be reported before reinsurance for columns 1 through 6.
- For columns 7 and 8, provide the number of in force standalone policies that are claims made vs. occurrence.
- Line 1.1 Provide the range of the limits offered for standalone policies.
- Line 2.2 Direct losses and defense and cost containment expenses for commercial multiple peril package policies are to be reported before reinsurance for Columns 1 through 4.
- For Columns 5 and 6, provide the number of in force multiple peril policies containing cybersecurity coverage that are claims made vs. occurrence.
- Line 2.4 If the answer to 2.3 is "yes," provide the amount of direct premium earned (qualified or estimated) for cybersecurity coverage included in package policies before reinsurance.
- Line 2.5 Provide the range of limits offered for the commercial multiple peril package cybersecurity policies
- Line 3.1 If the answer to 3 is yes, provide the range of limits offered for tail coverage.



MAURA HEALEY
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

May 14, 2015

The Honorable Jeb Hensarling
Chairman
The Committee on Financial Services
U.S. House of Representatives
Washington, DC 20215

The Honorable Maxine Waters
Ranking Member
The Committee on Financial Services
U.S. House of Representatives
Washington, DC 20215

Re: *Federal Legislation Relating to Data Security and Breach Notification Standards*

Dear Chairman Hensarling and Ranking Member Waters:

We write concerning the Committee's upcoming hearing, entitled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." We are encouraged and appreciate that the Committee recognizes the critical importance of this issue. In this era of increasing data breach risks, strong data security protections and breach disclosure requirements are essential to protect consumers and to preserve confidence in the market.

We understand that one issue before this Committee is whether federal data security and breach notification standards are warranted. We are cognizant of the business community's concerns regarding compliance with multiple state security breach notification regimes. As it considers this issue, we urge the Committee to carefully balance the calls for a national standard with the necessary protections consumers currently rely upon under state law, to avoid invalidating those critical protections and leaving consumers in a vulnerable position.

In particular, we write to share with the Committee the insights and perspective this Office has gained through its enforcement of Massachusetts' data security breach notification law,¹ data security regulations,² and data disposal law.³ Together, these laws (enforced by this Office through the Massachusetts Consumer Protection Act)⁴ require covered entities to develop, implement, and maintain minimum data security procedures and policies, consistent with

¹ Mass. Gen. Laws ch. 93H, attached as [Exhibit 1](#).

² Title 201 of the Code of Massachusetts Regulations ("CMR"), section 17.00 *et seq.*, attached as [Exhibit 2](#).

³ Mass. Gen. Laws ch. 93I, attached as [Exhibit 3](#).

⁴ Mass Gen. Laws ch. 93A.

industry standards, to safeguard Massachusetts consumers' "personal information"⁵ (whether in paper or electronic form) from anticipated threats or hazards and from unauthorized access or use.⁶ Massachusetts data breach notice law also obligates entities to provide notice as soon as reasonably practicable, and without unreasonable delay, to affected residents and state agencies in the event of a breach of security or compromise of that information.⁷

From September 1, 2007 through December 31, 2014, this Office received notice of over 9,800 data breaches, reporting over 5 million impacted Massachusetts residents. Over 2,400 breaches were reported in 2014 alone (a 33% increase over 2012 and a 527% increase over 2008). To the extent any of those breaches resulted in enforcement actions by this Office (a very small percentage), the circumstances reflected gross failures to implement or maintain basic security practices, unreasonable delays in providing notice of the breach, or other egregious conduct that raised real risks of resulting consumer harm. More commonly, this Office engages in regular outreach with the business community to improve data security practices and facilitate compliance with those laws. As a result of this work, this Office has an informed and comprehensive view into the nature, extent, and frequency of data breaches, the challenges businesses encounter, the risks faced by consumers and, most importantly, the security practices and procedures that can prevent or mitigate those risks.

Our experience reflects that data breaches are an ever-present and increasing threat for companies and consumers alike, that strong data security and data breach notification standards are essential, and that the States need to retain the ability to protect their consumers from these rapidly-evolving risks. In particular, we believe that any effective data security and breach notification framework should include the following features.

- **Federal Law Should Establish a "Floor," not a "Ceiling," of Consumer Protections.**

We appreciate the calls for a uniform, federal standard for data security and breach notice. But any such federal standard should not dilute or preempt protections already in place in many States, including Massachusetts. In order to raise the level of protection nationally, to enable the States to innovate to best protect the needs of their residents, and to avoid enacting a stagnant security and breach standard that fails to keep up with changing technologies, a federal standard should set a "floor" of protections that state law can exceed. To the extent Congress intends to preempt state law in this field, it should set standards that are at least as strong – or stronger – than the protections consumers currently rely upon in their states. Finally, the scope of any federal preemption should be narrowly and carefully drawn to avoid: preempting state laws in areas other than data security or breach notification, infringing on the States' consumer protection laws or enforcement authority, or preventing the States from continuing to innovate to protect their consumers from the rapidly evolving data security and privacy risks.

⁵ In Massachusetts, "personal information" is defined by statute to mean a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security number; or (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. See Mass Gen. Laws ch. 93H, §1.

⁶ See Mass Gen. Laws ch. 93I and 201 CMR 17.00 *et seq.*

⁷ See Mass Gen. Laws ch. 93H.

- **Federal Law Should Preserve and Respect the States' Enforcement Authority.**

Recent breaches reported in the media underscore the necessary role played by the state Attorneys General in enforcing data breach and data security requirements for the protection of consumers. Indeed, in enforcing Massachusetts data security and breach notification law over the past several years, this Office has developed specialized expertise in the highly technical and rapidly evolving field of data security, and an informed perspective on the causes and effects of data breaches and the data security practices that can best avoid or mitigate them. The offices of many other state Attorneys General have developed a similar expertise and perspective. To harness this collective expertise, and to ensure that state Attorneys General can continue their role of protecting their consumers, any federal standard should preserve the States' existing enforcement authority, and in particular, with respect to the following areas.

First, prompt notice of breaches to the relevant state Attorneys General in cases where their State's residents are impacted is imperative. If threshold numbers of affected consumers are set for state regulator notice, they should not be so high that it frustrates a State's ability to enforce the law with respect to the vast majority of breaches that impact its residents. For example, in Massachusetts, approximately 97% of the 2,314 data breaches reported in 2013 involved fewer than 10,000 persons; in fact, each of these breaches affected, on average, 74 persons. Thus, thresholds requiring notice to state regulators that exceed 100 residents of that State would thus frustrate this Office's ability to protect Massachusetts residents.

Second, a dual federal/state enforcement framework that respects – not constricts – the enforcement prerogatives of the States should be utilized. Provisions that give exclusive enforcement authority to federal agencies, restrict state Attorneys General to suits in federal courts or create new enforcement mechanisms or procedures risk injecting unnecessary delay, costs and complications for the States. Numerous federal laws illustrate that parallel or dual federal/state enforcement coordination of consumer protection laws is both possible and effective.⁸

Third, to protect their consumers, state Attorneys General must be able to seek adequate civil remedies, including where appropriate preliminary and permanent injunctive relief to compel compliance, civil penalties to deter misconduct, attorneys' fees/costs, and restitution for ascertainable losses suffered by consumers (remedies currently obtainable by this Office under the Massachusetts Consumer Protection Act). If "caps" on civil penalties are set, they should be meaningful enough to deter future misconduct, so as to not be treated as a cost of doing business. Moreover, because consumers are the ultimate victims of data breaches, they should retain the ability to bring private rights of action to seek recovery of damages or harm they may suffer.

⁸ See, e.g., the Federal Trade Commission Act (15 U.S.C. § 45(a)(1) and its numerous State counterparts (see, e.g. Mass Gen. Laws ch. 93A), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), and the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and Health Information Technology for Clinical and Economic Health (HITECH) Act (42 U.S.C. § 17930 *et seq.*).

- **Federal Law Should Enhance – Or At Least Preserve – Existing State and Federal Standards.**

State consumer protection and data security/breach notice laws provide important protections for consumers. As the Committee considers a national standard, it should build on these existing protections under federal and state law to ensure consumers are not exposed to increased risks as a result of a new national standard. In this vein, we urge the Committee to consider the following.

- **Data Security Standards Under Massachusetts and Federal Law Should Be Preserved.**

Massachusetts' data security regulations (201 CMR 17.00 *et seq.*) and its data disposal law (Mass Gen. Laws ch. 93I) represent one of the leading information security frameworks in the nation. Rather than employ a "one-size-fits-all" approach or an undefined, generalized standard of "reasonableness," Massachusetts utilizes a risk-based, process-oriented approach to data security, similar to well-established federal standards governing financial institutions and certain health-related entities.⁹ Covered entities must develop, implement, and maintain a written security program outlining administrative, technological, and physical safeguards appropriate for the entity's size, scope of business, amount of resources available to it, the nature and quantity of data collected or stored, and the need for security of the personal information it handles. Within this flexible framework, the regulations outline various categories of security measures and practices that constitute a "reasonable" information security program.

We believe that consumers will be best protected by a federal data security standard that is at least as comprehensive and strong as the Massachusetts data security regulations. Indeed, our review of thousands of breach notifications underscores the need for strong and enforceable data security standards. While some breaches result from intentional, criminal acts, many result from the failure to employ basic security practices, such as through the improper disposal of consumers' information, lost files, disclosure through inadvertence, carelessness, or the failure to follow basic and well-accepted data security practices. Often even those breaches resulting from intentional criminal attacks could reasonably have been avoided or mitigated if the entity had complied with its own data security policies or employed basic security practices such as software updates or firewalls.

⁹ Similar to existing federal standards applicable to financial institutions (*see* 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information)) and entities covered under HIPAA (*see e.g.* 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information)), Massachusetts requires entities to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information (201 CMR 17.03(2)(b)); develop, implement and maintain a "written comprehensive information security program" containing physical, administrative and technical safeguards necessary to protect personal information from those risks (201 CMR 17.03); take reasonable steps to oversee third parties handling personal information (201 CMR 17.03(2)(f)); and securely dispose of personal information (Mass Gen. Laws ch. 93I). Cognizant of the particular risks associated with electronic data, Massachusetts also requires entities, among other things, to establish and maintain a technically-feasible computer security system (201 CMR 17.04); and to encrypt personal information sent over public networks or wirelessly, or stored on laptops and portable devices (201 CMR 17.04(3), (5)).

A strong, generally-applicable standard would bolster the overall security of consumer data in commerce (and with it, consumer confidence), reduce the costs and burdens of responding to a data breach, and eliminate any potential competitive disadvantages created by differing, sector-specific standards. Further, the data security standard should not be so minimal so as to create a competitive disadvantage to those businesses that choose to invest in more robust, and more costly, data security measures in recognition of the inadequate protections resulting from such a minimal standard. To ensure that the law is responsive to changing technologies and risks, the Committee should consider giving rule-making authority to the Federal Trade Commission to define as appropriate those security measures and practices that are considered “reasonable.”

o Definitions of Protected Consumer Information Should Be Broad and Flexible, Not Narrow and Static.

In today’s data-driven economy, consumers share a variety of highly personal data points with numerous commercial entities. This information includes not just authenticating information that can lead directly to identity theft or fraud (such as biometric data, social security numbers, and drivers’ license numbers), but various other types of information that can be used to access financial accounts, perpetrate medical or tax identity theft or fraud, or cause emotional distress or physical harm against a consumer. This may include, for example, financial account numbers, online account log-in credentials (and/or the secret question and answers necessary to access those credentials), geolocation information, details about a consumer’s mental and physical health, personal habits, hobbies, shopping activity, political views, or religious beliefs. Such information can be used to identify a given consumer, obtain highly personal details about them, predict their future actions, and thus more convincingly impersonate them, or cause harm against them.

To encompass the various categories of information that can be used to impersonate or cause harm to a consumer and the changing nature of identity theft, the Commission should take this opportunity to adopt a broad and flexible statutory definition of protected “personal information,” and not be limited to existing federal or state statutory definitions. The Committee should further consider giving the Federal Trade Commission (“FTC”) rule-making authority to amend the definition of protected personal information as necessary to ensure it remains responsive to changing information practices and technologies.

o Consumers Must Be Promptly Notified of a Breach.

If preventing identity theft is the goal of a federal data breach notice standard, requiring timely notice of the breach to the consumer should be the first priority. Timely notice to the consumer may reduce the risk of resulting economic and noneconomic damages by enabling the consumer to take preemptive protective measures (such as by monitoring their credit reports and financial account records, placing security freezes or fraud alerts on their credit, and being on alert for identity theft or fraud). Conversely, delayed notice could increase the risk of both economic and non-economic harm by unduly shortening or eliminating the window of opportunity for such prophylactic steps.

Additionally, standards that require consumer notice only after the breached entity determines that there is a risk of financial harm to the consumer (so-called “financial harm triggers”) are problematic in at least three respects. First, connecting any specific breach to financial harm can be a difficult and time consuming process, and may not be possible depending on the circumstances of a particular breach. Second, allowing the company to conduct a risk assessment deprives the consumer of the ability to make their own determination of their own risk, and may prevent them from taking steps to mitigate that risk. Third, financial harm triggers fail to take into account non-financial harms that can occur, such as medical identity theft, professional or personal embarrassment, or loss of access to online accounts or services. A federal standard should instead require breach notification as soon as reasonably practicable and without unreasonable delay when an entity knows, or has reason to know, that protected personal information of a consumer has been acquired without authorization, or used for unauthorized purposes.

We applaud the Committee for tackling this difficult but critical issue, and appreciate the opportunity to share our expertise. We are happy to provide you with any information you may need and to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws. Please do not hesitate to contact us with questions you may have about the points raised above, or about this issue in general.

Sincerely,

/s/ Jonathan B. Miller
Jonathan B. Miller
Chief, Public Protection and Advocacy Bureau

Sara Cable
Assistant Attorney General
Consumer Protection Division

Office of Attorney General Maura Healey
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108
(617) 727-2200

May 21, 2015

US House of Representatives
Committee on Financial Services
Comments for the Record from the *Secure ID Coalition* pertaining to the full Committee hearing on
May 14, 2015
Protecting Consumers: Financial Data Security in the Age of Computer Hackers

Following the Committee's hearing on May 14, 2015 entitled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers", the Secure ID Coalition (SIDC) agreed it was important to provide clarification for the Record about smart card technology (also referred to in your hearing as chip based cards) and known as the EMV payment standard.

Founded in 2005, the Secure ID Coalition is a smart card industry coalition that works with industry experts, public policy officials, and federal and state agency personnel to promote identity policy solutions that enable both security and privacy protections. Because of our commitment to citizen privacy rights and protections we advocate for technology solutions that enable individuals to make decisions about the use of their own personal information. Coalition members subscribe to principles that include the deployment of secure identity solutions, advise on and advocate for privacy protections and enhanced security in all digital consumer applications including financial services, healthcare and homeland security.

Please find below points of clarification that we believe to be helpful to understanding smart card technology.

- Smart card technology, often called chip card technology, is a mature and proven security technology used for a wide variety of applications around the world. Today there are billions of security chip cards at work in a number of applications such as mobile SIM cards, healthcare cards, travel documents (including passports), secure access systems, transit cards and bank cards.
- Robust encryption, on a hardware based secure chip is the foundation for the new financial services cards being rolled out in the United States today. Early versions of chip cards were standardized by financial services industries in the United States and Europe in 1994 into the EMV Standard, used today in over 2 billion payment cards worldwide.
- The EMV transition in the US is underway to improve the security of payment cards by removing the vulnerability of magnetic stripe technology which can easily be accessed, manipulated and stolen with off-the-shelf equipment. In contrast, chip cards contain a secure chip which protects the card data and is capable of secure communication with point-of-sale terminals or readers.
- When using a chip based card the embedded microprocessor in the card enables security, and the point-of-sale terminal or card reader actually "talks" to the microprocessor. The microprocessor enforces access to the data on the card. When a transaction is complete the microprocessor generates a unique transaction code allowing the sale. This type of dynamic data makes it virtually impossible for fraudsters and criminals to counterfeit or hack. Further, it

makes any data stolen from a data breach useless to hackers, since they have no way of creating a new card with the stolen data.

- The most significant benefit of chip card security is the reduction in fraud resulting from counterfeit, lost and stolen cards. The EMV standard enables card authentication, cardholder verification and transaction verification, all features unavailable or lacking using magnetic stripe technology. In-person fraud is currently the largest payments fraud problem in the US market, according to the Financial Services Roundtable. Implementing chip based cards will go a long way toward reducing this type of fraud because these cards are nearly impossible to clone or copy.
- The US is the last G-20 nation to transition to chip based financial services cards, both Canada and Mexico have already implemented them along with Europe, Asia and most of South America. Because of the US' unique online verification system that provided some security for payment transactions, chip-based cards were slow to be adopted. As other nations began the transition to chip-based payment cards, eliminating fraud from cloned, copied or stolen cards, the fraud migrated to the US. The US continues to see an uptick in fraud resulting from data breaches making the move to chip based cards even more critical.
- Like computing power and each new edition of the iPhone, smart card chips increase in capacity and sophistication every year. Each year the capability of the smart card chip is better than the year before and incorporates more processing power and stronger security features to protect consumer transactions.
- Our industry works with leading research scientists and "white-hat" hackers to test the security of our products so we can stay ahead of the attackers. While multi-factor authentication solutions always create a more secure environment for customers, the transition to a chip-based card from a magnetic stripe is a significant improvement over the current technology in consumers' hands.
- SIDC supports all types of innovation in the payment market place, especially mobile payment technologies. Our members are continually working with the financial services industry to implement many of the future solutions for enhancing security and privacy protection. Credit and debit cards can be used, for the most part, anywhere in the world because all parties have agreed to common standards for operation. The next wave of technologies will go through a similar standards process to ensure consumers enjoy the same seamless experience. However, standards setting processes take time and won't happen overnight. In the meantime the common universal standard used today for payment is EMV.
- SIDC is also concerned about non-financial harm that consumers may face when certain types of information is breached, especially health information. Any legislation addressing data breaches should consider putting in place incentives for proactive solutions to protect consumer data. Notice of a data breach does little to help consumers after their data is already gone. While laws currently exist to protect consumers from losses resulting from fraudulent financial transactions, no such laws are in place for theft of healthcare data.

Cybersecurity risks are among the gravest threats facing Americans. Fraudsters and hackers threaten our personal livelihoods as well as our national security. Securing our financial infrastructure is one of the highest impact actions we can take to protect ourselves from criminals that seek to do us harm. The Secure ID Coalition applauds the House Financial Services Committee for looking at the issue of cyber threats to consumers. The SIDC fully supports the action of the financial services industry to move the US credit and debit card market to EMV chip-based cards in order to mitigate the harm from data attacks. EMV is a proven technology standard that ensures consumer security, privacy protection and global interoperability.

Additionally, SIDC members embrace mobile payment solutions and other emerging payment technologies, on which we are actively working to make such a future a reality. However, we are not yet at a point where such technologies can become the default option for all consumers. Implementation of EMV chip-based cards is not only the highest impact action we can currently undertake to reduce fraud and protect consumers, it is also the only truly egalitarian and democratic technology that can protect financial information and reduce fraud for all consumers here and now.

Responses from Jason Oxman to questions for the record submitted by Representative Bill Foster
Hearing entitled, "Protecting Consumers: Financial Data Security in the Age of Computer Hackers"
Financial Services Committee
May 14, 2015

Chip cards, often referred to as EMV cards, represent an important improvement in security at the retail point of sale. Specifically, EMV cards prevent the creation and use of counterfeit cards, which eliminates the single most common form of card fraud at retailers in the U.S. EMV cards are more secure than traditional magnetic stripe cards because the chip in the EMV card generates a unique, dynamic security code for each transaction, an improvement on the static, unchangeable security code on a magnetic stripe card. As a result of the dynamic security code in the EMV card, criminals cannot create a counterfeit card using stolen account information. EMV card transactions are transmitted to highly secure payments systems that are protected against breach, making electronic payments the safest and most reliable way to pay. And even if criminals are able to somehow intercept card numbers, EMV prevents counterfeit cards from being successfully used at retailers. In conjunction with tokenization and point to point encryption technologies that retailers and payments companies are deploying today, EMV cards will help the fight against criminal fraud. Chip card technology insulates against any single point of failure by deploying security technology that prevents criminals from creating and using counterfeit credit cards.



600 13th Street, NW
Suite 400
WASHINGTON, DC 20005
TEL 202-289-4322

www.FSRoundtable.org

July 16, 2015

The Honorable Bill Foster
United States House of Representatives
1224 Longworth House Office Building
Washington, DC 20515

Dear Congressman Foster:

Thank you for the question you submitted for the record following my testimony at the recent hearing titled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers." Specifically, you asked: "It seems that the ultimate barrier is not data security, but authentication. You discussed a variety of identity verification methods. Where is the market going?"

While effective authentication is a vitally important part of security, it is only one component of a more holistic and layered approach that is needed to improve data security. According to a recent study¹, the most common causes of data breaches are malicious or criminal attacks, which utilize malware, system infections, insider threats and more. Such threats are difficult to thwart with effective authentication alone. Nonetheless, it is also clear that human carelessness remains a significant initial pathway for breaches. In such instances, effective authentication can prevent or reduce breach risks.

A recent survey² found "123456" and "password" remain two of the most popular password choices for consumers. For security professionals, this discouraging news emphasizes the need to move beyond traditional, static authentication methods that incentivize cyber criminals to continue to target consumer accounts that too often have weak or exposed credentials in the form of a password or Personal Identification Number (PIN).

Innovations in authentication enhance consumer protections, and present opportunities for financial institutions to increase security, reduce fraud, and foster a frictionless user experience for their customers across various channels of interaction. "Multi-factor authentication" techniques add at least one additional layer of identity verification beyond basic log-on credentials like a username and password and such techniques are now being widely adopted.

¹ "2014 Cost of Data Breach Study: United States." Ponemon Institute, May 2014.

² <http://splashdata.com/press/worst-passwords-of-2014.htm>

Many financial institutions have also augmented these capabilities by using “out-of-band” protocols that require a text message containing a one-time use code being sent to a customer’s on-file mobile number. This significantly increases the institution’s confidence in the customer’s identity.

In addition, authentication techniques depicted in movies not long ago are now moving closer to becoming possible options. Examples include biometric, gesture, location and other identification techniques.

The financial industry is innovating and developing new authentication practices and identity management techniques at a rapid pace. While changes may require consumers to adapt to new authentication processes, the changes will result in less fraud, greater security, and consumers’ continued trust in the financial sector to keep their data safe.

Thank you for the question, and for your service to our country. If you or your staff have additional questions or would like to discuss these topics further, please contact Jason Kratovil, FSR’s head of payments policy, at (202) 589-1931.

Sincerely,

A handwritten signature in black ink, appearing to read 'T. Pawlenty', with a stylized flourish at the end.

Tim Pawlenty
Chief Executive Officer



Jim Nussle
President & CEO

601 Pennsylvania Ave., N.W.
South Building, Suite 600
Washington D.C. 20004-2601

Phone: 202-508-6745
Fax: 202-438-7734
jnussle@cuna.coop

May 13, 2015

The Honorable Jeb Hensarling, Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Maxine Waters, Ranking
Member
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Hensarling and Ranking Member Waters:

On behalf of the Credit Union National Association (CUNA), I am writing to thank you for holding a hearing entitled "Protecting Consumers: Financial Data Security in the Age of Computer Hackers"¹ which will address the importance of protecting consumer data. CUNA is the largest credit union advocacy organization in the United States, representing America's state and federally chartered credit unions and their 102 million members.

Credit unions take the protection of their members' personal and financial information very seriously. Unfortunately, many recent breaches of retailers and other non-regulated businesses have shown that not all of those in the payments system feel the same way. These major breaches have cost credit unions, which are owned by their members, millions of dollars. We urge Congress to address this problem head-on.

The Data Security Act of 2015

Representatives Neugebauer and Carney recently introduced H.R. 2205, the "Data Security Act of 2015." CUNA strongly supports this legislation. Protecting consumer information is a shared responsibility of all parties involved in a payments transaction. This important legislation ensures all entities that handle consumers' sensitive financial data have in place a robust process to protect data, which can help prevent breaches from happening in the first place.

Stopping data breaches is critical for consumers, and also important to credit unions, who often have the closest relationship with the affected consumers. Data breaches impose significant costs on credit unions and other financial institutions of all sizes because our first priority is to protect consumers by blocking fraudulent transactions and making their accounts whole. Credit unions provide relief to card holders that are victims of breaches, regardless of where the data breach occurs.

This important legislation would apply to all industries that handle sensitive financial or personal information and would provide meaningful and consistent protection for consumers nationwide. H.R. 2205 recognizes that it is not necessary or productive to duplicate data protection and consumer notice requirements that are already in place for financial institutions under the Gramm-Leach-Bliley Act (GLBA)¹ and other relevant regulations. Credit unions already have a system in place that protects sensitive nonpublic personal information and it makes sense to extend similar requirements to other industries that handle sensitive consumer information. H.R. 2205 requires

¹ Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (1999).

The Honorable Jeb Hensarling
The Honorable Maxine Waters
May 13, 2015
Page Two

merchants to meet comparable standards. This is necessary to provide the best possible protections for consumers.

The reforms in H.R. 2205 would effectively replace the current patchwork of state and federal regulations for data breaches with a national law that provides uniform protections across the country. This comprehensive approach would better serve consumers by making it easier for businesses and government agencies to take the steps necessary to adequately protect all Americans from identity theft and account fraud.

Costs of Data Breach

Data breaches impose significant costs on banks, credit unions and other financial institutions of all sizes. Following a data breach that occurs at a retailer, credit unions' first priority is to protect members and make them whole. Credit unions immediately take steps to protect their members including: notifying their members, determining whether to reissue debit and credit cards, increasing call center staff, setting up account monitoring, and conducting other defensive activities. These steps are not done without a cost, much of which is not reimbursed. For the not-for-profit credit unions operating on already thin margins, these costs make a significant difference in their bottom line and therefore in their ability to offer services to their members.

Over the past few years, media attention has been drawn to a number of large-scale breaches at retailers such as: Target, Home Depot, Michaels, TJX and others. CUNA has conducted research on the cost to credit unions from these breaches.

- The Target breach alone is estimated to have affected 5.4 million cards and cost credit unions over **\$30 million**.
- The size of the Home Depot breach exceeded even the Target breach with an estimated 7.2 million cards affected. Total costs to credit unions from the breach came in at more than **\$57 million**. The estimate cost per affected card breaks down as follows:
 - Card reissuance: \$2.64 per affected card.²
 - Fraud: \$4.89 per affected card.
 - All other costs: \$0.50 per affected card.
 - Total costs: \$8.02 per affected card.

² These are costs averaged across all affected cards, not just cards that have been reissued.

The Honorable Jeb Hensarling
The Honorable Maxine Waters
May 13, 2015
Page Three

These data breaches did not occur in isolation. Unfortunately, many merchant data breaches occur at smaller retailers outside of the national spotlight, and every time a breach occurs credit unions bear the costs of making members whole.

All participants of the payments system should share the responsibility of protecting consumer data, and when a data breach occurs the entity responsible for the breach should incur the costs of the breach. To that end, CUNA is advocating a proactive solution (H.R. 2205) to help those without sufficient standards in place, to establish those standards so the overall number of breaches and the number of affected consumers drops drastically.

GLBA Standards for Financial Institutions are Strong

H.R. 2205 excludes credit unions from its provisions, recognizing that subjecting them to the standards in this bill would be unnecessary and duplicative. Financial institutions, including credit unions, are already subject to robust data security standards under the GLBA. The National Credit Union Administration (NCUA), implements data security standards for credit unions, as does the Federal Financial Institutions Examination Council (FFIEC).

Some industries—including the financial services industry—are required by law to develop and maintain robust internal protections to combat and address criminal attacks, and are required to protect consumer financial information and notify consumers when a breach occurs within their systems that will put their customers at risk. The same cannot be said for other industries, like retailers, that routinely handle this same information and increasingly store it for their own purposes.

Specifically, under section 501(b)³ of GLBA, Congress required NCUA and other federal financial regulators to establish standards to ensure financial institutions protect the security and confidentiality of the nonpublic personal information of their members or customers.

NCUA's regulations implementing section 501(b) of GLBA and other security rules, requires credit unions to establish a comprehensive data security program addressing the safeguards for customer records and information.⁴ These safeguards are intended to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against any unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer. In addition, these regulations require credit unions to develop and implement "risk-based" response programs to address instances of unauthorized access to member information.

³ 15 U.S.C. 6801(b).

⁴ 12 C.F.R. Part 748.

The Honorable Jeb Hensarling
The Honorable Maxine Waters
May 13, 2015
Page Four

Data security requirements under the GLBA and NCUA's regulations are subject to the supervision and enforcement of NCUA for federal credit unions or the state supervisory agencies for federally-insured state-chartered credit unions. Additionally, the Federal Trade Commission has enforcement authority for compliance with these requirements for state-chartered credit unions.

Scalability of GLBA for Financial Institutions

Under GLBA standards, financial institutions are required to have risk-based information security programs in place to safeguard consumers' personal and financial information, and respond to instances of unauthorized access to confidential data. The federal financial institution regulators have made clear that each institution's information security program is scalable to the size and complexity of the institution and the nature and scope of its activities. Therefore, every bank and credit union can customize its security program to suit the needs of the institution and the consumers it serves.

Like GLBA, H.R. 2205 would require "non-banks" that handle consumers' sensitive information to develop and maintain effective information security programs tailored to the complexity and scope of a company's operations. The bill would accommodate companies of all sizes while fulfilling the need for a single set of national data security standards.

Regulatory Oversight is Firmly in Place for Financial Institutions

In addition to the strong standards credit unions maintain under the GLBA, they are also subject to regulation by NCUA on data and cybersecurity. NCUA and other federal regulators have many regulations and best practices in place along with examination resources to ensure that financial institutions use state-of-the-art data security practices. Further, in the financial services industry, data and cybersecurity is a team effort. The regulators, including NCUA, are members of the FFIEC.

Financial regulators are doing a lot of work on cybersecurity. One example of NCUA's dedication to cybersecurity is its cybersecurity resource page,⁵ which details all of NCUA's cybersecurity efforts and resources for credit unions. The FFIEC conducted a cybersecurity assessment in 2014 on 500 community financial institutions. This assessment analyzed risk and preparedness at these institutions. FFIEC member regulators will use information learned through the assessment to update current guidance, aligning it with changing cybersecurity risks.

NCUA and the other bank regulators' data and cybersecurity efforts are too voluminous to detail here, but span the array of regulations, best practices and examination. The regulators' joint cybersecurity efforts through the FFIEC demonstrate the leadership that the financial services industry has taken to ensure that all types of institutions fall under stringent regulation and best practices. Moreover, compliance is tested by regulators on an ongoing basis, which helps to ensure that regulations and

⁵ Available at <http://www.ncua.gov/Resources/Pages/cyber-security-resources.aspx>.

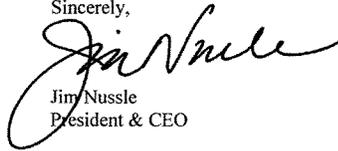
The Honorable Jeb Hensarling
The Honorable Maxine Waters
May 13, 2015
Page Five

best practices are appropriate and implemented correctly for maximum effectiveness. Because credit unions are subject to GLBA standards and supervision by NCUA, they already must adhere to safeguards aimed at protecting consumer data.

As the House Financial Services Committee considers data security legislation this Congress, we encourage you to ignore the excuses, attempts to pass blame, and efforts to make this a fight between business sectors. The debate on data security should be about protecting sensitive financial information, ensuring consumers feel confident that their data is secure, whether it's where they shop or at their financial institution. We encourage this Committee to support and pass H.R. 2205 which would make all members of the payments system subject to equally diligent standards for data security and ultimately ensure consumers' information is safe.

Thank you again for your leadership on data security and for allowing us to submit testimony for the record. We look forward to working with Congress on this important issue.

Sincerely,



Jim Nussle
President & CEO



STATEMENT OF

DAVID FRENCH

SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS
NATIONAL RETAIL FEDERATION

FOR THE HOUSE FINANCIAL SERVICES COMMITTEE

HEARING ON

“PROTECTING CONSUMERS: FINANCIAL DATA SECURITY IN THE
AGE OF COMPUTER HACKERS”

MAY 14, 2015

National Retail Federation
1101 New York Avenue, NW
Suite 1200
Washington, DC 20005
(202) 626-8126
www.nrf.com

Chairman Hensarling, Ranking Member Waters, and members of the Committee on Financial Services, on behalf of the National Retail Federation (NRF), I want to thank you for the opportunity to respectfully submit this statement for the hearing record and provide you with our views on cybersecurity threats facing the private sector and achievable solutions that Congress and the White House may work toward in order to better protect Americans' financial information.

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

We appreciate the committee calling this hearing at a time when all different kinds of American businesses find themselves the targets in an evolving war on our digital economy – a war in which we are unwilling combatants who must defend vigorously against attacks by both criminals and nation states. Key aspects of the cyber attacks facing the breadth of American industries are, typically, the criminal fraud motive and the foreign source of the attack. Virtually all of the data breaches we have seen in the United States during the past year – from attacks on the networked systems of retail, entertainment and technology companies that have been prominent in the news, to a reported series of attacks on our largest banks last summer – have been perpetrated by overseas criminals who are breaking the law. All of these breached companies are victims of these foreign-actor crimes, and we should keep this in mind as we explore the issues discussed at the hearing and in forthcoming public policy initiatives relating to this issue.

Retailers collectively spend billions of dollars safeguarding sensitive customer information and fighting fraud that results when criminals succeed in breaching their protected information systems. Data security is something that our members place at the top of their business priorities, and securing data from increasingly sophisticated attacks is an effort that retailers, as a community, strive to improve every day. This is also an issue on which the retailer and consumer interests are aligned in protecting some of the most sensitive information retailers hold – typically, the customer's payment card number. If retailers are not good custodians of payment data related to our customers, they will no longer continue to frequent our establishments and use their credit and debit cards in our stores. When we examine the threats to all businesses, we should understand the basic underlying reason that retailers are being attacked is for payment card numbers in order to perpetrate credit card fraud.

We also urge members of the Committee to review and support legislative efforts designed to help mitigate the threat of cyber attacks as well as inform consumers of breaches of sensitive information whenever and wherever they occur. These issues are ones that we recommend you examine in a holistic fashion: we need to help prevent cyber attacks, and when attacks result in data breaches, help reduce fraud or other economic harm that may result from those breaches. We should not be satisfied with simply determining what to do after a data breach occurs – that is, who to notify and how to assign liability. Instead, it is important to look at why such breaches occur, and what the perpetrators get out of them, so that we can find ways to reduce and prevent not only the breaches themselves, but the follow-on harm that is often the

criminal motive behind these attacks. If breaches become less profitable to criminals, then they will dedicate fewer resources to committing them, and our data security goals will become more achievable.

With these three guiding observations in mind, below are six proposed solutions that would help businesses defend against cyber attacks and mitigate the harm from any resulting breaches of security. These are proposals that we believe policymakers can work together to achieve in the near term, either through consumer and industry-supported legislation, or by working with the private sector on improving security practices outside of the lawmaking process. We begin by providing our views below on the evolving nature of the cybersecurity threat, and the latest data showing that this threat is not unique to any one industry. Following that, we discuss our six-point proposal and some of the technological advancements retailers have promoted that could improve the security of our networks. We also offer additional ways to achieve greater payment security since the payment card data itself is what drives the attacks on the retail industry. Additionally, in our proposed solutions, we suggest some of the elements of data breach notification legislation that may provide the best approach to developing a uniform, nationwide notification standard, based on the strong consensus of state laws, which would apply to all businesses that handle sensitive personal information of consumers.

A. Cyber Attacks and Data Breaches in the United States

Unfortunately, cyber attacks and data breaches are a fact of life in the United States, and virtually every part of the U.S. economy and government is being attacked in some way. In its recently released 2015 Data Breach Investigations Report,¹ Verizon determined there were 79,790 data security incidents reported by industry and public institutions in 2014, and that 2,122 of those had confirmed data losses. Of those, public institutions (including governmental entities) had 14.3%, the financial industry had 13.1%, manufacturing had 11.1%, accommodations providers (including hotels and restaurants) had 10.5%, retailers had 7.7%, healthcare providers had 6.6%, and information industries (including software publishers, cable providers, telecommunications providers, and data processing and related services combined) had 4.5%.

The latest breach report data from Verizon reflects that significantly more data breaches (with confirmed data losses) occur at financial institutions than at retailers. Criminals are after the most valuable information they can find, and payment card numbers – which are immediately cancelled and replaced with new numbers when fraud is discovered – are not as valuable as bank account information that can lead to account takeovers and/or identity theft. It should also be noted that even these percentage figures above obscure the fact that there are far more merchants that are potential targets of criminals in this area, as there are one thousand times more merchants accepting card payments in the United States than there are financial institutions issuing cards and processing those payments. It is not surprising, then, that data thieves focus far more often on banks, which hold our most sensitive financial and personal information – including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.

¹ 2015 Data Breach Investigations Report by Verizon, available at: <http://www.verizonenterprise.com/DBIR/2015/>

These figures are sobering. There are far too many attacks that result in data breaches, and the breaches are often difficult to detect and are carried out in many cases by criminals with the latest technological methods at their disposal and significant resources behind them. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality. It is also a key reason why our proposed solutions below focus on the payment card system and hardening protections against card fraud. Without fraud-prone payment card information in a retailer's system, criminals would not find the rest of the information retailers hold – benign data such as phone book information, shoe size, color preference, etc. – to be all that interesting, or more importantly, lucrative on the black market.

B. Achievable Solutions to Improving Cybersecurity

As noted above, protecting their businesses and customers from cyber attacks is of paramount importance to retailers. In today's world of networked systems, the retail industry also recognizes that it is going to take the highest level of collaboration and coordination to make sure we do it right. That means government, industry and law enforcement alike must work together to address and defend against the attacks facing American businesses. As part of our efforts to build this collaboration necessary to succeed, NRF's President and Chief Executive Officer, Matt Shay, and Vice President for Retail Technology, Tom Litchford, were on hand at The White House Summit on Cybersecurity and Consumer Protection, held at Stanford University on February 13, 2015. President Obama announced new steps there to combat an increasing number of cyber attacks that have hit targets ranging from retail stores to insurance companies to the White House itself. As the president remarked, "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information, as true partners."

We agree and support President Obama's call for cybersecurity threat information-sharing as a necessary element of any set of proposals to defend against cybersecurity attacks. NRF supports the passage by the House of legislation like H.R. 1560, the "Protecting Cyber Networks Act," sponsored by Rep. Devin Nunes, which passed the House of Representatives with strong, bipartisan support reflected in a recorded vote of 307-116. This type of legislation would protect and create incentives for private sector entities to lawfully share cyber-threat information with other private entities and with the federal government in real-time. This would help companies better defend their own networks from cyber attacks detected elsewhere.

NRF also commended the goals of the president's Executive Order, which called for establishing cyber threat information-sharing among non-critical infrastructure industries through Information Sharing and Analysis Organizations (ISAOs). The information-sharing groups proposed by President Obama appear similar to the Information Technology Security Council formed by NRF last year that currently shares cyber threat information among nearly 170 security professionals, such as Chief Information Security Officers (CISOs), from over 100 of the most influential retail companies. NRF has partnered with private sector and government entities to develop and disseminate cybersecurity threat indicators to our members. These partners include the Financial Services Information Sharing and Analysis Center (FS-ISAC), the United States Computer Emergency Readiness Team (US-CERT) of the Department of Homeland Security, the United States Secret Service (USSS), and the Federal Bureau of Investigation (FBI). More than 2,000 cyber threat alerts have been sent to our participating retail

members since the inception of our threat information-sharing program, and we continue to expand its reach among the retail community.

In an open letter to the president that NRF published during the summit, we applauded the White House and President Obama for providing solution-based leadership around the significant threat posed by hackers and other cyber criminals. We also affirmed the retail industry's commitment to safeguarding consumer data and working with the president and Congress to achieve practical solutions to these serious problems. Our letter outlined a specific set of additional, achievable solutions that we – and every industry with a stake in the issue – must work toward in order to better protect American consumers, empower our businesses and effectively safeguard America's cyberspace against criminal hackers. Specifically, we called upon policymakers to work toward these solutions beyond the information-sharing efforts noted above:

- Support the immediate passage of **FEDERAL FRAUD PROTECTION FOR DEBIT CARDS**, similar to what we enjoy for credit cards. Americans should not have to pay more for fraud protection.
- Call on the payment card industry to stop relying on fraud-prone signatures and issue **PIN AND CHIP CARDS** for all Americans, among the least protected consumers in the world.
- Encourage all entities in the payments system — not just retailers — to **ADOPT END-TO-END ENCRYPTION** to protect consumers' payment information throughout the entire payments chain.
- Endorse the development of **OPEN, COMPETITIVE TOKENIZATION STANDARDS** to replace consumers' sensitive personal data (including payment card data) with non-sensitive "tokens" so that stored information is useless to would-be hackers.
- Continue support for a **SINGLE NATIONAL DATA BREACH NOTIFICATION LAW** that would establish a clear disclosure standard for all businesses to inform consumers of breaches whenever and wherever they occur.
- Support the passage of federal law enforcement legislation that would **AID IN THE INVESTIGATION AND PROSECUTION OF CRIMINALS** that breach our businesses' networks and harm our consumers.

In reviewing these proposals, we ask that you consider our views in each of these six areas of achievable solutions:

1. Federal Fraud Protection for Debit Cards

From many consumers' perspective, payment cards are payment cards. As has been often noted, consumers would be surprised to learn that their legal rights, when using a debit card

– i.e., their own money – are significantly less than when using other forms of payment, such as a credit card. It would be appropriate if policy makers took steps to ensure that consumers' reasonable expectations were fulfilled, and they received at least the same level of legal protection when using their debit cards as they do when paying with credit.

NRF strongly supports bipartisan legislation like S. 2200, the “Consumer Debit Card Protection Act,” cosponsored by Senators Warner and Kirk last Congress. S. 2200 was a bipartisan solution that would immediately provide liability protection for consumers from debit card fraud to the same extent that they are currently protected from credit card fraud. This is a long overdue correction in the law and one concrete step Congress could take immediately to protect consumers that use debit cards for payment transactions.

2. Payment Card Security – “PIN and Chip” Cards

There are many technologies available that could reduce fraud resulting from payment card breaches, and an overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. That is because using the best network security technology and practices available does not guarantee that a business can avoid suffering a security breach which exposes sensitive data, such as payment card numbers. Therefore, raising security standards alone may not be the most efficient or effective means of preventing potential harm to consumers from card fraud. With respect to payment card numbers, for example, it is possible that no matter how much security is applied by a business storing these numbers, the numbers may be stolen from a business's database in a highly sophisticated security breach that can evade even state-of-the-art system security measures. Because of these risks, it makes sense for industry to do more than just apply increased network or database security measures.

One method to help prevent downstream fraud from stolen card numbers is to require more data or additional numbers from a consumer (such as their entry of a 4-digit personal identification number, or “PIN”) to complete a payment transaction rather than simply permit the transaction to be approved on the basis of the numbers that appear on the face of a card. Requiring this type of out-of-wallet information in order to authorize and complete payment card transactions is time-tested by the banking industry, as they have required the use of PINs to access bank accounts through ATM machines for decades, a minor inconvenience that American consumers have borne for the trade-off in increased security when accessing cash. Around the globe, the most industrialized nations – the G-20 – have also adopted PIN-based solutions to replace the antiquated signature authentication methods that derive from the mid-twentieth century.

NRF believes it is time to phase out signature-authentication for all U.S.-issued payment cards – today's magnetic stripe cards as well as tomorrow's chip-based cards – and adopt a more secure authentication method for credit and debit card transactions. PINs can provide an extra layer of security against downstream fraud even if the card numbers (which the card companies already emboss on the outside of a card) are stolen in a breach. In PIN-based transactions, for example, the stored 20-digits from the card would, alone, be insufficient to conduct a fraudulent transaction in a store without the 4-digit PIN known to the consumer and not present on the card itself. These business practice improvements are easier and quicker to implement than any new federal data security law, and they hold the promise of being more effective at preventing the

kind of financial harm that could impact consumers as companies suffer data security breaches affecting payment cards in the future.

In support of these concepts, on October 17, 2014, the President signed an executive order initiating the BuySecure Initiative for government payment cards.² The order provided, among other things, that payment cards issued to government employees would include PIN and chip technology and that government equipment to handle and process transactions would be upgraded to allow acceptance of PIN and chip. Requiring PINs for all payment card transactions, as are required for some debit and ATM transactions (and some in-bank teller transactions as well) are common-sense actions that the banking industry should adopt immediately. Retail customers – American consumers – would be better protected by the replacement of a signature – a relic of the past – with the tried-and-true PIN that all other G-20 nations, including Canada, the U.K. and our European allies have adopted as part of their card payment system to protect their citizens.

As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This approach to payment card security should be adopted not only in the brick-and-mortar environment, in which a physical card is used, but also in the online environment in which the physical card does not have to be used. Many U.S. companies, for example, are exploring the use of a PIN for online purchases, similar to efforts underway already in Canada and Europe. Adopting PIN-like protections for online purchases may help directly with the 90 percent of U.S. fraud which occurs online.

3. Network Security – “End-to-End Encryption”

Encryption of payment card transaction data is another technological solution retailers employ to help defend against cyber attacks and that could help deter and prevent data breaches and the resulting fraud that can occur. Merchants are already required by Payment Card Industry (PCI) data security standards to encrypt cardholder data while being stored but, as not everyone in the entire payments chain is able to accept data in encrypted form during payment authorization, sensitive data may be left exposed (after it leaves the retailer’s system in encrypted form) at a critical time in the payment process. Payment security experts have therefore called for a change to require “end-to-end” (or “E2E”) encryption, which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the payment card data in encrypted form. This would require, as the PCI standards currently require of merchants but not of others in the payment stream, that card-issuing banks, merchant banks, branded payment card networks and payment card processors all adopt the same technology to handle encrypted payment card data. In fact, knowing that card chip technology alone is not the panacea touted by branded payment card networks, many retailers are not waiting for an E2E standard, and are investing, at significant costs, in point-to-point (or “P2P”) encryption.³

² Executive Order – Improving the Security of Consumer Financial Transactions, The White House, October 17, 2014. Accessible at: <http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>

³ NRF Retail CIO Download, Agenda 2015: Secure and Innovate, February 2015, page 12

According to the September 2009 issue of the Nilson Report “most recent cyber attacks have involved intercepting data in transit from the point of sale to the merchant or acquirer’s host, or from that host to the payments network.” The reason this often occurs is that “data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can’t accept encrypted data at this time.”⁴

Keeping sensitive data encrypted throughout the payments chain would go a long way to convincing fraudsters that the data is not worth stealing in the first place – at least, not unless they were prepared to go through the arduous task of trying to de-encrypt the data which would be necessary in order to make use of it. We ask policymakers to urge our partners in the payments system, like we have, to adopt the most secure technologies to protect American consumers from card fraud. In the meantime, until all of the stakeholders in the payments system adopt technology to enable “end-to-end” encryption, using PIN-authentication of payment cards now would offer some additional protection against fraud should the decrypted payment data today be intercepted by a criminal during its transmission “in the clear.”

4. Open, Competitive Tokenization Standards

Another sensible and achievable proposal to deter and protect against the harm that may result from cyber attacks is to minimize the storage and use by businesses of the full set of unredacted and unencrypted payment card numbers necessary to complete a transaction – a data protection principle known as “data minimization.” For example, a decade ago, the National Retail Federation asked the branded card networks and banks to lift the requirement that retailers store full payment card numbers for all transactions.

Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the “token”). Sensitive payment card data can be replaced, for example, with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.⁵ Still, like the other proposed technological solutions above, tokenization is not a silver bullet solution, and it is important that whichever form of tokenization is adopted be one based on an open standard. This would help prevent a small number of networks from obtaining a competitive advantage, by design, over other payment platforms through the promotion of proprietary tokenization standards only.

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers would not need to have a physical payment card – and the mobile payments technology certainly would not need to replicate the security problem of physical cards that emboss account numbers on their face. It should also be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords, and increasingly, biometric finger prints. Indeed, if we are looking to leapfrog the already aging and fraud-prone current technologies, mobile-driven payments may be the answer.

⁴ The Nilson Report, Issue 934, Sept. 2009 at 7.

⁵ For information on Shift4’s 2005 launch of tokenization in the payment card space see <http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lets-merchants-re-use-credit>.

As much improved as they are, the proposed chips to be slowly rolled out on U.S. payment cards are essentially dumb computers. Their dynamism makes them significantly more advanced than magnetic stripes on most of American's payment cards today, but their sophistication pales in comparison with the sophistication of even the most basic and common smartphone. Smartphones contain computing powers that could easily enable state-of-the-art fraud protection technologies. In fact, "the new iPhones sold over the weekend of their release in September 2014 contained 25 times more computing power than the whole world had at its disposal in 1995."⁶ Smart phones soon may be nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

5. National Data Breach Notification Law

The Year of the Breach, as 2014 has been nicknamed, was replete with news stories about data security incidents that raised concerns for all American consumers and for the businesses with which they frequently interact. Criminals focused on U.S. businesses, including merchants, banks, telecom providers, cloud services providers, technology companies, and others. These criminals devoted substantial resources and expertise to breaching the most advanced data protection systems. Vigilance against these threats is necessary, but we need to focus on the underlying causes of breaches as much as we do on the effects of them.

If there is anything that the recently reported data breaches have taught us, it is that any security gaps left unaddressed will quickly be exploited by criminals. For example, the failure of the payment cards themselves to be secured by anything more sophisticated than an easily-forged signature makes the card numbers particularly attractive to criminals and the cards themselves vulnerable to fraudulent misuse. Likewise, cloud services companies that do not remove data when a customer requests its deletion, leave sensitive information available in cloud storage for thieves to later break in and steal, all while the customer suspects it has long been deleted. Better security at the source of the problem is needed. The protection of Americans' sensitive information is not an issue on which unreasonably limiting comprehensiveness makes any sense.

In fact, the safety of Americans' data is only as secure as the weakest link in the chain of entities that share that data for a multitude of purposes. For instance, when information moves across communications lines – for transmission or processing – or is stored in a "cloud," it would be senseless for legislation to exempt these service providers, if breached, from comparable data security and notification obligations to those that the law would place upon any other entity that suffers a breach. Likewise, data breach legislation should not subject businesses handling the same sensitive customer data to different sets of rules with different penalty regimes, as such a regulatory scheme could lead to inconsistent public notice and enforcement.

Given the breadth of these invasions, if Americans are to be adequately protected and informed, federal legislation to address these threats must cover all of the types of entities that handle sensitive personal information. Exemptions for particular industry sectors not only ignore the scope of the problem, but create risks criminals can exploit. Equally important, a single federal law applying to all breached entities would ensure clear, concise and consistent notices to all affected consumers regardless of where they live or where the breach occurs.

⁶ "The Future of Work: There's an app for that," *The Economist* (Jan. 3, 2015).

Indeed, Congress could establish the same data breach notice obligations for *all* entities handling sensitive data that suffer a breach of security. Congress should not permit “notice holes” – the situation where certain entities are exempt from reporting known breaches of their own systems. If we want meaningful incentives to increase security, everyone needs to have skin in the game.

The chart below, however, illustrates how some breach bills, such as H.R. 2205, sponsored by Rep. Randy Neugebauer and cosponsored by Rep. John Carney, Jr., would operate with respect to notice by either banks or other “third-party entities” operating in the payment system. This graphic illustrates a typical payment card transaction in which a payment card is swiped at a card-accepting business, such as a retail shop, and the information is transmitted via communications carriers to a data processor, which in turn processes the data and transmits it to the branded card network, such as Visa or MasterCard, which in turn processes it and transmits it to the card-issuing bank. (Typically there also is an acquirer bank adjacent to the processor in the system, which the chart omits to provide greater clarity of the general payment flows.)



H.R. 2205 would only require the retail shop, in this example, to provide consumer notice of a breach of security. The payment data processor, transmitter (telecommunications carrier) or card company suffering a breach would qualify as a third-party whose only obligation, if breached, is to notify the retail shop of their breach – not affected consumers or the public – so that the retailer provides notice on their behalf. And the bank suffering a breach would be exempt from the notification obligations to consumers or the public under H.R. 2205.

Compared to the figures in Verizon's 2015 Data Breach Investigations Report noted above, this consumer notice regime presents an inaccurate picture of the breadth of breaches to consumers.⁷ Furthermore, such a notice regime is fraught with possible over-notification because payment processors and card companies are in a one-to-many relationship with retailers. If the retailers must bear the public disclosure burden for every other entity in the networked payment system that suffers a breach, then 100% of the notices would come from the entities that suffer less than 8% of the breaches. This is neither fair nor enlightened public policy.

Financial Institution Exemptions

Many legislative proposals this Congress have "notice holes," where consumers would not receive disclosures of breaches by certain entities. Perhaps the notice hole that has been left unplugged in most proposals, including H.R. 2205, is the exemption from notification standards for entities subject to the Gramm Leach Bliley Act (GLBA), which itself does not contain any statutory language that requires banks to provide notice of their security breaches to affected consumers or the public. Interpretive information security guidelines issued by federal banking regulators in 2005 did not address this lack of a requirement when it set forth an essentially precatory standard for providing consumer notice in the event banks or credit unions were breached. Rather, the 2005 interagency guidelines state that banks and credit unions "should" conduct an investigation to determine whether consumers are at risk due to the breach and, if they determine there is such a risk, they "should" provide consumer notification of the breach.⁸ These guidelines fall short of creating a notification requirement using the language of "shall," an imperative command used in proposed breach notification legislation for entities that would be subject to Federal Trade Commission enforcement. Instead, banks and credit unions are left to make their own determinations about when and whether to inform consumers of a data breach.

Several accounts in 2014 of breaches at the largest U.S. banks demonstrate the lack of any notice requirement under the interagency guidelines. It was reported in news media last fall that as many as one dozen financial institutions were targeted as part of the same cyber attack scheme.⁹ It is not clear to what extent customers of many of those institutions had their data compromised, nor to our knowledge have the identities of all of the affected institutions been made public. The lack of transparency and dearth of information regarding these incidents reflects the fact that banks are not subject to the same requirements to notify affected customers of their own breaches of security as other businesses are required now under 47 state laws and would be required under most proposed federal legislation, despite the fact that financial institutions hold Americans' most sensitive financial information. A number of the more seasoned and robust state laws, such as California's breach notification law, have not exempted financial institutions from their state's breach notification law because they recognize that banks are not subject to any federal requirement that says they "shall" notify customers in the event of a breach of security.

⁷ <http://www.verizonenterprise.com/DBIR/2015/>

⁸ Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS), accessible at: <https://www.fdic.gov/news/news/financial/2005/fil2705.html>

⁹ "JP Morgan Hackers Said to Probe 13 Financial Firms," *Bloomberg* (Oct. 9, 2014).

General Principle for Notification

With respect to establishing a national standard for individual notice in the event of a breach of security at an entity handling sensitive personal information, the only principle that makes sense is that these breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of their own systems. Just as the Federal Trade Commission (FTC) expects there to be reasonable data security standards employed by each business that handles sensitive personal information, a federal breach notification bill should apply notification standards that “follow the data” and apply to any entity in a networked system that suffers a breach of security when sensitive data is in its custody. With respect to those who have called upon the entity that is “closest to the consumer” to provide the notice, we would suggest that the one-to-many relationships that exist in the payment card system and elsewhere will ultimately risk having multiple entities all notify about the same breach – someone else’s breach. This is not the type of transparent disclosure policy that Congress has typically sought. An effort to promote relevant notices should not obscure transparency as to where a breakdown in the system has occurred. Indeed, a public notice obligation on all entities handling sensitive data would create significant incentives for every business that operates in our networked economy to invest in reasonable data security to protect the sensitive data in its custody. By contrast, a federal law that permits “notice holes” in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public’s trust.

Data Security Standards

Data security standards vary depending on the nature of an entity’s business and where it operates. Over the past half-century, the United States has essentially taken a sector-specific approach to data privacy (including data security) requirements, and our current legal framework reflects this. For example, credit reporting agencies, financial institutions, and health care providers, just to name a few regulated sectors, have specific data security standards that flow from laws enacted by Congress, such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), respectively.

The agencies that have implemented section 501(b) of GLBA—the Federal Financial Institutions Examination Council (FFIEC), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (Fed Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS)—have defined a process-based approach to security in the *Interagency Guidelines Establishing Information Security Standards* (“Security Guidelines”)¹⁰ Under the Security Guidelines, however, when designing security controls a financial institution is required to design an information security plan that “controls the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope” of the entity’s activities and, in so doing, must consider certain security measures and only if appropriate, adopt them.¹¹ Significantly, one of these security measures that a financial

¹⁰ Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS).

¹¹ *Id.* at ¶ III, C.1.

institution must consider, but is not required to adopt, is a “response program that specify actions to be taken when the institution suspects or detects that *unauthorized individuals have gained access to customer information systems*, including appropriate reports to regulatory and law enforcement agencies.”¹² (*emphasis added*)

Those operating in other industry sectors that are subject to the jurisdiction of the Federal Trade Commission (FTC) must abide by the standards of care enforced by the FTC under Section 5 of the FTC Act, which give the Commission broad, discretionary authority to prosecute “unfair or deceptive acts or practices” (often referred to as their “UDAP” authority). On top of this federal statutory and regulatory framework, states have regulated businesses’ data security practices across a variety of industry sectors and enforced consumer protection laws through their state consumer protection agencies and/or their attorneys general.

Legal exposure for data security failures is dependent on the federal or state laws to which a business may be subject and is alleged to violate. The FTC, for example, has been very active in bringing over 50 actions against a range of companies nationwide that are not otherwise subject to a sector-specific federal data security law (e.g., GLBA, HIPAA, etc.). For example, under its Section 5 UDAP authority, the FTC has brought enforcement actions against entities that the Commission believes fall short in providing “reasonable” data security for personal information. Nearly all of these companies have settled with the FTC, paid fines for their alleged violations (sometimes to the extent of millions of dollars), and agreed to raise their security standards and undergo extensive audits of their practices over the next several decades to ensure that their data security standards are in line with the FTC’s order.

Effect of Imposing GLBA-Like Standards with FTC Enforcement

NRF supports federal data security standards for all entities handling sensitive consumer information, but federal standards to be enforced by the FTC against the wide range of businesses under its jurisdiction would fall under the Commission’s broad and discretionary authority to prohibit “unfair or deceptive acts or practices” and should be enforced consistent with the Commission’s long-standing practices under Section 5 of the FTC Act. This standard is consistent with the consumer protection standard that applies to financial institutions. Under Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the Consumer Financial Protection Bureau (CFPB) was established and granted the authority to prohibit “unfair, deceptive or abusive acts or practices” for consumer financial products and services.¹³ As the CFPB explains in the CFPB Supervision and Examination Manual, “Unfair, deceptive, or abusive acts and practices (UDAAPs) can cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace.”¹⁴ NRF is not aware of any financial institutions that have suggested that the CFPB standard is too weak.

Providing the FTC with different authority – to enforce process-based data security standards like those in the Security Guidelines implementing GLBA – would be an unprecedented and dramatic expansion of the FTC’s authority that is unjustified in its application

¹² *Id.* at ¶ III, C.1.g.

¹³ The text of the Act is available at: <http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf>

¹⁴ CFPB Supervision and Examination Manual, Version 2, October 2012, p. 174 (UDAAP 1), available at: http://www.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf

to the broad array of businesses subject to its jurisdiction. The Security Guidelines were designed for banking regulators that take an audit/examination approach to regulating companies and work with them through an iterative process to help the institution come into compliance where it may be lacking, without the threat of severe penalties. The FTC, by contrast, takes an enforcement approach, which under a GLBA-like guidelines standard, would require a post-hoc determination of a company's compliance with an amorphous standard in a world where the technological threat vectors are ever-changing.

In an adversarial investigatory process, like the kind the FTC employs in its enforcement of Section 5 of the FTC Act, entities are either guilty or not, and more likely to be guilty by the mere fact of a breach. Unlike financial institutions subject to the Security Guidelines, companies subject to FTC enforcement of its UDAP authority are not able to get several bites at the apple working with regulators until they know they are in compliance with the regulator's vision of data security. Rather, businesses facing FTC enforcement would have to guess at what will satisfy the agency and, if their security is breached, the strong enforcement presumption would be that the company failed to meet the subjective standard.

Because of this disparity in how security guidelines would be enforced, NRF sought an expert opinion on the effect of federal legislation, such as the recently introduced H.R. 2205, that would impose banking industry-based data security standards on a vast array of commercial businesses, ranging from large nationwide companies to small, single-location businesses that are not "financial institutions." This would include every non-banking business in America that accepts virtually any form of tender other than cash (e.g., credit cards, debit cards, checks, etc.) in exchange for goods and services. As part of your efforts to examine this issue, we strongly encourage you to review the white paper – attached as *Appendix A* to this testimony – that was prepared by two former associate directors responsible for financial and credit practices in the FTC's Bureau of Consumer Protection and released in March. The authors' analysis provides a valuable perspective to the Committee and indicates why we believe the broad expansion of data security standards similar to the GLBA guidelines to virtually every unregulated business in the U.S. economy would be a dramatic expansion of regulatory authority that is unprecedented in its scope and unjustified in its application.

Finally, the different enforcement regimes between financial institutions and entities subject to the FTC's jurisdiction is also evident in the manner and frequency with which fines are assessed and civil penalties imposed for non-compliance with a purported data security standard. Banks are rarely (if ever) fined by their regulators for data security weaknesses. But, as noted above, commercial companies have been fined repeatedly by the FTC. Providing an agency like the FTC, with an enforcement approach, a set of standards with significant room for interpretation is likely to lead to punitive actions that are different in kind and effect on entities within the FTC's jurisdiction than the way the standards would be utilized by banking regulators in an examination. A punitive approach to companies already victimized by a crime would not be appropriate nor constructive in light of the fact that the FTC itself has testified before Congress that no system – even the most protected one money can buy – is ever 100% secure.

Preemption – Establishing a Nationwide, Uniform Standard of Notification

For more than a decade, the U.S. federalist system has enabled every state to develop its own set of disclosure standards for companies suffering a breach of data security and, to date, 47

states and 4 other federal jurisdictions (including the District of Columbia and Puerto Rico) have enacted varying data breach notification laws. Many of the states have somewhat similar elements in their breach disclosure laws, including definitions of covered entities and covered data, notification triggers, timeliness of notification, provisions specifying the manner and method of notification, and enforcement by state attorneys general. But they do not all include the same requirements, as some cover distinctly different types of data sets, some require that particular state officials be notified, and a few have time constraints (although the vast majority of state laws only require notice “without unreasonable delay” or a similar phrase.)

Over the past ten years, businesses such as retailers, to whom all the state and federal territory disclosure laws have applied, have met the burden of providing notice, even when they did not initially have sufficient information to notify affected individuals, through standardized substitute notification procedures in each state law. However, with an increasingly unwieldy and conflicting patchwork of disclosure laws covering more than 50 U.S. jurisdictions, it is time for Congress to acknowledge that the experimentation in legislation that exists at the state level and that defines our federalist system has reached its breaking point, and it is time for Congress to step in to create a national, uniform standard for data moving in interstate commerce in order to ensure uniformity of a federal act’s standards and consistency of their application across jurisdictions.

For years, NRF has called on Congress to enact a preemptive federal breach notification law that is modeled upon the strong consensus of existing laws in nearly every state, the District of Columbia, Puerto Rico and other federal jurisdictions. A single, uniform national standard for notification of consumers affected by a breach of sensitive data would provide simplicity, clarity and certainty to both businesses and consumers alike. Importantly, a single federal law would permit companies victimized by a criminal hacking to devote greater attention in responding to such an attack to securing their networks, determining the scope of affected data, and identifying the customers to be notified, rather than diverting limited time and resources to a legal team attempting to reconcile a patchwork of conflicting disclosure standards in over 50 jurisdictions. In sum, passing a federal breach notification law is a common-sense step that Congress should take now to ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.

Preemption of state laws and common laws that create differing disclosure standards is never easy, and there is a long history of Supreme Court and other federal courts ruling that, even when Congress expresses an intent to preempt state laws, limiting the scope of the preemption will not result in preemption. All it will accomplish is to add yet another law, this time federal, to the state statutes and common laws already in effect, resulting in the continuation of a confusing tapestry of state law requirements and enforcement regimes. A federal act that leaves this in place would undermine the very purpose and effectiveness of the federal legislation in the first place.

In order to establish a uniform standard, preemptive federal legislation is necessary. But that does not mean (as some have contended) that the federal standard must or should be “weaker” than the state laws it would replace. On the contrary, in return for preemption, the federal law should reflect a strong consensus of the many state laws. Some have called for a more robust notification standard at the federal level than exists at the state level. Without adding unnecessary bells and whistles, NRF believes that Congress can create a stronger breach

notification law by removing the exemptions and closing the types of “notice holes” that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses. This approach would enable members that are concerned about preempting state laws to do so with confidence that they have created a more transparent and better notification regime for consumers and businesses alike. It is a way this Congress can work to enact a law with both robust protection and preemption.

We urge Congress, therefore, in pursuing enactment of federal breach notification legislation, to adopt a framework that applies to all entities handling sensitive personal information in order to truly establish uniform, nationwide standards that lead to clear, concise and consistent notices to all affected consumers whenever or wherever a breach occurs. When disclosure standards apply to all businesses that handle sensitive data, it will create the kind of security-maximizing effect that Congress wishes to achieve.

Essential Elements of Data Breach Notification Legislation

In summary, a federal breach notification law should contain three essential elements:

- **Uniform Notice:** Breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of their own systems. A federal law that permits “notice holes” in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – unfairly burdens the former and unnecessarily betrays the public’s trust.
- **Express Preemption of State Law:** A single, uniform national standard for notification of consumers affected by a breach of sensitive data would provide simplicity, clarity and certainty to both businesses and consumers alike. A federal breach law would be a common-sense step to ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.
- **Reflect the Strong Consensus of State Laws:** A national standard should reflect the strong consensus of state law provisions. Congress can create a stronger breach notification law by removing the exemptions and closing the types of “notice holes” that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses, similar to the comprehensive approach Congress has taken in previous consumer protection legislation that is now federal law.

6. Greater Investigation and Prosecution of Cyber Criminals

In addition to the marketplace and technological solutions suggested above, NRF would also support a range of legislative solutions that we believe would help improve the security of our networked systems and ensure better law enforcement tools to address criminal intrusions.

Most important among these legislative solutions would be efforts to strengthen our extra-territorial law enforcement. As noted in our introduction above, industry sectors across the U.S. share the collective concern and face the same threat to their businesses’ networks that

appear to come predominantly from foreign actors. If the U.S. economy were threatened by foreign actors that had the most sophisticated technology to counterfeit our U.S. dollars, and were using it to perpetrate fraud in the United States and disrupt our economy, would Congress only be asking the victimized companies that accepted counterfeit cash as payment why they did not better protect their customers from this fraud? We think that Congress, in this hypothetical, would look first toward the criminal actors and enterprises that were perpetrating these crimes on our shores.

We therefore call upon Congress to develop legislation that would provide more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches – particularly those with foreign attack signatures – are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

C. Conclusion

American retailers are targets of cybercrime and suffer nearly 8% of all security breaches predominantly because of the payment card data they accept and process. Criminals desire U.S.-based card numbers because they are unprotected and easily sold on the global black market to would-be fraudsters. The data thieves and their criminal customers – the purchasers of these stolen card numbers – realize the short lifespan of stolen card numbers once a breach is detected. This is why the criminals that hack American businesses typically go to extraordinary lengths to mask their incursions with methods that have not been seen before and that are not addressed by network security solutions. In short, if they can act undetected in this “cat-and-mouse” game, and place stolen card numbers on the black market before law enforcement and victimized businesses know the cards are there, they can drive up the market price for the stolen cards.

As stated earlier, retailers have invested billions in adopting data security technology. Efforts to promote payment card security, end-to-end encryption and tokenization are highlighted in the discussion above. The dominant card networks and card-issuing banks, however, have not made all of the technological improvements suggested above to make the payment cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe. Our ability to improve payment card security and protect American consumers in the chain of the American payment ecosystem is, and will only be, as strong as its weakest link. Without the cooperation of our partners in the financial system, we cannot alone affect the changes necessary to better defend and protect against cyber attacks that lead to payment card fraud. Everyone already has skin in the game, and we need to work together to do what we can to improve an aging and outdated payment system that is the principal target of cyber attacks affecting U.S. retail businesses and their customers.

While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft that result from cyber attacks, there is much left for card-issuing banks and payment card networks to contribute, as retailers are doing, to better protect our payment system and the fraud-prone cards that are used in them. That is why we have proposed practical, commonsense and achievable solutions above that NRF believes are necessary to helping deter and defend against cyber attacks affecting the retail industry. We appreciate the opportunity to submit this statement to the committee today, and we look forward to working

with the members of the committee on bringing greater attention to these issues and helping push forward some or all of our proposed solutions to address these important concerns.

Appendix A:

NRF White Paper on Data Security

The Effect of Applying Customer Information Safeguard Requirements for Banks
to Nonfinancial Institutions

Joel Winston and Anne Fortney

March 2015

We have been asked to analyze the effect of legislation requiring the Federal Trade Commission (“FTC”) to apply standards based upon the Interagency Guidelines for banks in Safeguarding Customer Information (“Interagency Guidelines” or “Guidelines”) to any entity that accepts bank-issued payment cards for goods and services and does not extend credit itself.

Summary

The Interagency Guidelines for Safeguarding Customer Information apply to depository institutions (“banks”) subject to supervisory examination and oversight by their respective regulatory agencies. The Guidelines contain detailed elements of an information safeguards program tailored specifically to banks. They are designed to be a point of reference in an interactive process between the banks and their examiners, with emphasis on compliance on an on-going basis. The FTC has issued a Safeguards Rule applicable to the nonbank “financial institutions” under its jurisdiction. The Safeguards Rule provides for more flexibility and less specificity in its provisions than do the Guidelines. The more general requirements of the FTC’s Rule are designed to be adaptable to ever-changing security threats and to technologies designed to meet those threats.

The differences in the approaches to data security regulation between the Guidelines and the FTC Safeguards Rule reflect two fundamental differences between the bank regulatory agencies (the “Agencies”) and the FTC: the substantial differences in the types and sizes of entities within the jurisdiction of the Agencies versus the FTC, and the equally substantial differences in the roles played by the Agencies and the FTC in governing the behavior of those entities. With respect to the former, while the banks covered by the Guidelines are relatively homogeneous, extending the Guidelines to all entities that accept payment cards would sweep in a vast array of businesses ranging from large multinational conglomerates to small operations, and could also include individuals.¹ The threats faced by these widely diverse businesses are likely to vary widely as well, as would the sophistication and capabilities of the entities themselves for addressing the threats. A flexible approach as in the Safeguards Rule is necessary to account for those critical differences. Many of the Guidelines’ provisions, which were drafted with banks in mind, likely would be unsuitable for a significant proportion of the entities that would be subject to these new requirements.

¹ Because of the near-universal acceptance of bank-issued cards as payment for goods and services, companies that would be subject to the Guidelines’ standards would include merchants, hotels, bars and restaurants, theaters, auto dealers, gas stations, grocery and convenience stores, fast-food eateries, airlines and others in the travel industry, hospitals and doctors, dentists, veterinarians, hair salons, gyms, dry cleaners, plumbers and taxi drivers. In other words, virtually all providers of consumer goods and services would be covered.

For similar reasons, the different approaches the Agencies and the FTC take in regulating their entities make it problematic to apply the Guidelines to the nonbank entities overseen by the FTC. The more specific Guidelines make sense when, as is the case with the banks, there is an ongoing, interactive dialogue between the regulated entities and the regulator through the supervision process. The regulated entities and regulators can address changes in threats and technologies during the less formal examination process and head-off potential problems before they happen. By contrast, the Safeguards Rule's flexible requirements are better suited to a law enforcement agency like the FTC that obtains compliance not by an interactive dialogue, but by prosecuting violations after-the-fact. Indeed, an entity within the FTC's jurisdiction may have no indication of deficiencies in its compliance until it is under investigation. With the untold numbers of entities potentially subject to its jurisdiction, the FTC simply lacks the capability or resources to engage in dialogue or provide the individualized, ongoing guidance like the Agencies do with their banks.

While the Guidelines would be made applicable to any entity that accepts bank-issued payment cards,² the Guidelines' specific requirements are suitable only for the bank card-issuers that dictate the card processing equipment and procedures for businesses that accept their cards, as well as the security features inherent in the cards. If the Guidelines were made applicable to businesses that merely accept banks' cards, they would impose security obligations on those with the least ability to implement the requirements applicable to payment card security.

Finally, nonbank businesses are subject to the FTC's general authority under the FTC Act to prohibit unfair or deceptive practices, and the FTC has prosecuted many companies under this authority for failing to protect consumer's nonpublic information. Subjecting nonbank businesses to the Guidelines' specific requirements would not enhance the FTC's ability to use its existing authority to protect consumers through enforcement actions. When it issued consumer information privacy and safeguards rules under the Gramm-Leach-Bliley Act, the FTC considered applying the rules to retailers that accept bank credit or debit cards and declined to do so. We believe that determination remains equally justified today.

Our Qualifications

Joel Winston served for 35 years in the FTC's Bureau of Consumer Protection. For nine years, he headed the FTC's offices responsible for consumer information privacy and security, serving as Associate Director for Financial Practices (2000-2005) and for Privacy and Identity Protection (2005-2009). His responsibilities included the development of the FTC Safeguards Rule in 2000-2001, and he directed the FTC's enforcement of that Rule and other consumer protection laws.

² Bank-issued payment cards include credit cards, debit cards and prepaid cards.

Anne Fortney has 39 years' experience in the consumer financial services field, including directing FTC enforcement and rulemaking under the federal consumer financial protection laws as the Associate Director for Credit Practices of the Bureau of Consumer Protection.

We both regularly counsel consumer financial services clients on their compliance obligations. We also assist clients in Consumer Financial Protection Bureau ("CFPB") examinations and in the defense of FTC and CFPB investigations and enforcement actions. In addition, we have each testified multiple times as invited witnesses before U.S. Congressional Committees and Subcommittees on various consumer financial protection laws. We each serve from time to time as subject matter experts in litigation in the federal courts involving consumer financial services.

Background

Federal Requirements for Safeguarding Customer Information

Section 501(b) of the Gramm-Leach Bliley Act ("GLBA" or the "Act")³ required each of the federal bank regulatory agencies (the "Agencies")⁴ and the FTC to establish standards for the financial institutions subject to their respective jurisdictions with respect to safeguarding consumers' nonpublic, personal financial information. The Act required that the safeguards ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.⁵

Interagency Guidelines

Because they exercise supervisory responsibilities over banks through periodic examinations, the Agencies issued their GLBA customer information safeguard standards in the form of Guideline document ("Interagency Guidelines" or "Guidelines").⁶

The Guidelines instruct banks on specific factors that serve as the basis for the Agencies' review during supervisory examinations. They are predicated on banks' direct control over the security of their customers' nonpublic personal financial information.

³ Gramm-Leach-Bliley Financial Modernization Act, Pub. L. 106-102, § 501(b) (1999), codified at 15 U.S.C.A. § 6801(b).

⁴ These were the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS"). In October 2011, as a result of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the OTS was terminated and its functions merged into the OCC, FRB, and FDIC.

⁵ 15 U.S.C.A. § 6801(b).

⁶ Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616-01 (Feb. 1, 2001) and 69 Fed. Reg. 77610-01 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (FRB); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). The Agencies later issued an interpretive Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736-01 (Mar. 29, 2005). This paper includes this interpretive Interagency Guidelines in the summary of the Interagency Guidelines.

They instruct each bank to implement a comprehensive written information security program, appropriate to its size and complexity, that: (1) insures the security and confidentiality of consumer information; (2) protects against any anticipated threats or hazards to the security or integrity of such information; and (3) protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Guidelines provide specific instructions for banks in the development and implementation of an information security program. A bank must:

- Involve the Board of Directors, which must approve the information security program and oversee the development, implementation and maintenance of the program;
- Assess risk, including reasonably foreseeable internal and external threats, the likelihood and potential damage of these threats, and the sufficiency of the bank's policies and procedures in place to control risk;
- Design the program to control identified risks. Each bank must consider whether the following security measures are appropriate for the bank, and, if so, adopt the measures it concludes are appropriate:
 - Access controls on customer information systems;
 - Access restrictions at physical locations containing customer information;
 - Encryption of electronic customer information;
 - Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
 - Dual control procedures,
 - Segregation of duties, and employee background checks for employees responsible for customer information;
 - Response programs that specify actions to be taken when the bank suspects or detects unauthorized access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
 - Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards;
- Train staff to implement the information security program;
- Regularly test key controls, systems, and procedures of the information security program;
- Develop, implement, and maintain appropriate measures to properly dispose of customer information and consumer information;
- Adequately oversee service provider arrangements, including by contractually requiring service providers to implement appropriate procedures and monitoring service providers;
- Adjust the program in light of relevant changes in technology, sensitivity of consumer information, internal and external threats, the bank's own changing business arrangements, and changes to customer information systems;
- Report to the Board of Directors at least annually; and

- Provide for responses to data breaches involving sensitive customer information,⁷ which should include –
 - Developing a response program as a key part of its information security program, which includes, at a minimum, procedures for assessing the nature and scope of an incident;
 - Notifying the bank’s primary federal regulator as soon as the bank becomes aware of the breach;
 - Notifying appropriate law enforcement authorities;
 - Containing and controlling the incident to prevent further unauthorized access to or use of consumer information; and
 - Notifying consumers of a breach when the bank becomes aware of an incident of unauthorized access to sensitive customer information. The notice must include certain content and must be given in a clear and conspicuous manner and delivered in any manner designed to ensure the customer can reasonably be expected to receive it.

FTC Safeguards Rule⁸

The FTC protects consumers against “unfair and deceptive acts and practices in or affecting commerce.”⁹ Its jurisdiction includes “all persons, partnerships, or corporations,” except banks, savings and loan institutions, federal credit unions and certain nonfinancial entities regulated by other federal agencies.¹⁰ The FTC issues substantive rules, such as the Safeguards Rule, when required by Congress to do so,¹¹ but it is not authorized to conduct supervisory examinations of entities under its broad jurisdiction. Rather, the FTC is primarily a law enforcement agency.

Because the FTC lacks supervisory examination authority, it issued a Safeguards Rule, rather than Guidelines, to establish customer information safeguards for “financial institutions” under its jurisdiction. The GLBA’s broad definition of “financial institution” includes a myriad of nonbank companies that operate in the consumer financial services industry.¹² The definition includes finance companies, auto dealers, debt collectors and consumer reporting agencies,

⁷ Sensitive customer information includes: a customer’s name, address, or telephone number, in conjunction with the customer’s social security number, driver’s license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer’s account, and any combination of components of customer information that would allow someone to log onto or access the customer’s account (i.e., user name and password, or password and account number). 12 C.F.R. Part 30, app. B, supp. A, § III.A.1; 12 C.F.R. Part 208, app. D-2, supp. A, § III.A.1, and Part 225, app. F, supp. A, § III.A.1; 12 C.F.R. Part 364, app. B, supp. A, § III.A.1; and 12 C.F.R. Part 570, app. B, supp. A, § III.A.1.

⁸ FTC Safeguards Rule, 16 CFR Part 314. The FTC issued the final rule in 2001.

⁹ 15 U.S.C.A. § 45(a)(1). The FTC Act also prohibits unfair methods of competition in or affecting commerce.

¹⁰ 15 U.S.C.A. § 45(a)(2). For example, the FTC Act exempts not-for-profit entities and common carriers subject to the Communications Act of 1934.

¹¹ The FTC has more general rulemaking authority under Section 18 of the FTC Act, 15 U.S.C.A. § 57a, but has promulgated very few rules under that section in recent years.

¹² See 15 U.S.C.A. § 6809(3) (defining “financial institution” to include any institution engaging in “financial activities”); 12 U.S.C.A. § 1843(k) (defining “financial activities” broadly to include activities that are “financial in nature or incidental to such financial activity” or “complementary to a financial activity”).

among many others. The FTC determined that the final Rule would not apply to retailers that merely accept payment cards, but rather, only to those that extend credit themselves, and only then to the extent of their credit granting activities.¹³

In recognition of the great variety of businesses covered by the Safeguards Rule, the FTC developed a rule that provided for flexible safeguard procedures that could be adapted to the myriad ways in which covered entities are structured and operate. The FTC Rule requires a financial institution to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the entity's size and complexity, the nature and scope of its activities, the types of risks it faces, and the sensitivity of the customer information it collects and maintains. The information security program must: (1) ensure the security and confidentiality of consumer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

In its development, implementation, and maintenance of the information security program, the financial institution must:

- Designate an employee or employees to coordinate the program;
- Identify reasonably foreseeable internal and external risks to data security and assess the sufficiency of safeguards in place to control those risks in each relevant area of the financial institution's operations (i.e., employee training, information systems, prevention/response measures for attacks);
- For all relevant areas of the institution's operations, design and implement information safeguards to control the risks identified in the risk assessment, and regularly test and monitor the effectiveness of key controls, systems, and procedures;
- Oversee service providers, including by requiring service providers to implement and maintain safeguards for customer information; and
- Evaluate and adjust the program in light of material changes to the institution's business that may affect its safeguards.

¹³ See 16 C.F.R. §§ 314.2(a) (adopting the Privacy Rule's definition of "financial institution"). That definition includes examples of "financial institutions," among them: retailers that extend credit by issuing their own credit cards directly to consumers; businesses that print and sell checks for consumers; businesses that regularly wire money to and from consumers; check cashing businesses; accountants; real estate settlement service providers; mortgage brokers; and investment advisors. 16 C.F.R. § 313.3(k)(2). The FTC also opined that debt collectors are "financial institutions." 65 Fed. Reg. 33646; 33655 (May 24, 2000). Further, the Privacy Rule also gives examples of entities that are *not* "financial institutions": retailers that only extend credit via occasional "lay away" and deferred payment plans or accept payment by means of credit cards issued by others; retailers that accept payment in the form of cash, checks, or credit cards that the retailer did not issue; merchants that allow customers to "run a tab"; and grocery stores that allow customers to cash a check or write a check for a higher amount than the grocery purchase and obtain cash in return. *Id.* at (k)(3).

When it promulgated this rule, the FTC considered requiring more specific and detailed data security requirements, but determined that doing so would have imposed significant regulatory burdens in light of the broad range of entities potentially subject to the Safeguards Rule.

Comparison of the Interagency Guidelines and the FTC Rule

Both the Interagency Guidelines and the FTC Rule apply only to “financial institutions” with respect to the “nonpublic personal” financial information they collect and maintain. Unlike the Guidelines, however, the FTC Rule applies to many types of entities whose principal business may not involve the provision of financial services to consumers.

While the Guidelines and the FTC Rule share some common elements, they differ in critical respects. In particular, the Interagency Guidelines, which are tailored to closely supervised and regulated banks, are much more detailed in their requirements. These requirements are designed to be the point of reference in an interactive process between the banks and their examiners. As their name implies, the Guidelines are intended to guide banks’ compliance on a going forward basis.

In contrast, the FTC Rule is significantly less specific in its data security requirements than the Guidelines, because the Rule applies to a much broader and more diverse group of entities with wider variations in the data they collect and maintain, the risks they face, and the tools they have available to address those risks. The more general requirements of the FTC Rule also are designed to be adaptable to the near-constant changes in threats, security technologies, and other evolutionary developments in this extremely dynamic area. Whereas the Agencies can address new developments through the interactive examination process, the FTC only has the blunt instrument of law enforcement. And, whereas the Agencies actively supervise and monitor the activities of the entities they oversee, the FTC can only investigate and, if appropriate, take enforcement action against a fraction of the entities over which it has jurisdiction. The FTC’s primary focus is on prosecuting past or existing deficiencies, and a company may receive no advance warning of a possible violation of the Safeguards Rule until it is confronted with an adversarial investigation. The Agencies’ goal, on the other hand, is to prevent future deficiencies by working with the bank on an ongoing basis.

Effect of an FTC Standard That Would Apply Interagency Guidelines to Nonbanks That Do Not Extend Credit and Only Accept Credit Cards

For several reasons, safeguards requirements designed for closely supervised banks that issue credit and debit cards are a poor fit for the vast array of entities that accept credit cards and debit cards as payment for their goods and services. First, as explained above, the Guidelines are premised on an ongoing and interactive process between regulator and regulated entity, whereby examiners can instruct a bank on an apparent failure to meet a specific requirement. This process enables the institution to explain why a particular element of the Guidelines may be inapplicable or to correct any real deficiencies without legal sanctions.

No such process is possible for entities subject to FTC oversight. The FTC obtains compliance by initiating law enforcement investigations, using compulsory process, when it suspects a potential law violation based on facts that have come to its attention. This “after the fact” review focuses, through an adversarial process, on the legal requirements or prohibitions that may have been violated. If violations are found, the FTC seeks a formal order prohibiting the illegal conduct and, in appropriate cases, imposing fines or redress to injured consumers. The FTC lacks supervisory examination authority and lacks the resources to provide the specific guidance and ongoing oversight that would be necessary to effectuate Guidelines-type rules covering the huge diversity of nonbank entities. The result would be comparable to the widespread confusion and noncompliance that resulted from the FTC’s attempt to so broadly define “creditors” subject to its Red Flags Rule¹⁴ that the Rule would apply to types of businesses (such as plumbers, dry cleaners, hospitals, and restaurants) for which the Rule requirements made little sense. Congress had to correct that result with legislation that “reined in” the FTC by limiting the rule to the kinds of “creditors” that need written procedures to detect and prevent identity theft, rather than virtually every consumer-facing business.¹⁵

Second, many of the specific requirements of the Guidelines simply are not relevant to, or would impose unreasonable obligations on, nonbanks. For example, with respect to credit and debit cards, the Guidelines’ obligations are premised on the specific circumstances and capabilities of card *issuers*, which differ substantially from those of entities that accept cards as payment. It is the card issuers, and not the card-accepting merchants, be they hotels or veterinarians, that dictate the card processing capabilities of the equipment and procedures that merchants must use, as well as the security features inherent in the cards. Although chip and PIN technology could reduce card fraud, and many retailers have demonstrated a willingness to install terminals to accept cards with that technology, only card-issuing financial institutions can decide whether to issue fraud-resistant chip and PIN cards. Were the FTC required to enforce safeguard standards for credit and debit card data based on the Guidelines’ model, it would be imposing obligations on the entities with the least ability to ensure that they were carried out.

Finally, it is important to note that nonbanks, although not covered by the Safeguards Rule, are subject to the FTC’s general authority under Section 5 of the FTC Act to prohibit unfair or deceptive practices. The FTC has used this authority to prosecute dozens of nonbanks for engaging in the same practices proscribed by the Safeguards Rule, i.e., failing to take reasonable measures to protect consumers’ personally identifiable information.¹⁶ Thus, it is unclear what

¹⁴ See 16 C.F.R. Parts 681.1(b)(4), (5) (2009) (effective until February 11, 2013) (referring to 15 U.S.C.A. § 1691a(r)(5) (the Equal Credit Opportunity Act), which defines “creditor” as, among other things, “any person who regularly extends, renews, or continues credit,” and defines “credit” as “the right granted by a creditor to a debtor to... *purchase property or services and defer payment therefor*”) (emphasis added).

¹⁵ Red Flag Program Clarification Act of 2010, Pub. L. 111-319, § 2 (2010).

¹⁶ See, e.g., *FTC v. Wyndham Worldwide Corp., et al.*, No. CV 12-1365-PHX/PGR, in the U.S. District Court for the District of Arizona (2012); *In the Matter of Fandango, LLC*, Matter Number 132 3089 (2014); *In the Matter of Cbr Systems, Inc.*, Matter Number: 112 3120 (2013); *In the Matter of Dave & Buster’s, Inc.*, Matter Number 082 3153

additional benefit to the public would gain by subjecting nonbanks to specific requirements of the Guidelines.

As noted earlier, when issuing the GLBA rules, including the Safeguards Rule, the FTC specifically considered whether the rules should apply to retailers that accept bank-issued credit cards but do not extend credit themselves. The FTC correctly concluded that to do so would constitute a significant expansion of the FTC's authority to encompass the regulation of any transaction involving acceptance of a payment, whether cash, cards, checks or otherwise.

(2010); *In the Matter of CVS Caremark Corp.*, Matter Number: 072-3119 (2009); *In the Matter of Gencia Corp. and Compgeeks.com d/b/a computer Geeks Discount Outlet and Geeks.com*, Matter Number: 082 3113 (2009); *In the Matter of TJX Companies*, Matter Number: 072-3055 (2008); *In the Matter of Life is good, Inc. and Life is good Retail, Inc.*, Matter Number: 0723046 (2008); *U.S. v. ValueClick, Inc., et al.*, No. CV 08-01711, in the U.S. District Court for the Central District of California (2008); *In the Matter of Guidelines Software, Inc.*, Matter Number: 062 3057 (2007); *In the Matter of CardSystems Solutions, Inc.*, Matter Number: 052 3148 (2006); *In the Matter of DSW Inc.*, Matter Number: 052 3096 (2006); *In the Matter of BJ's Wholesale Club, Inc.*, Matter Number: 042 3160 (2005); *In the Matter of Petco Animal Supplies, Inc.*, Matter Number: 0323221 (2005); *In the Matter of Guess?, Inc. and Guess.com, Inc.*, Matter Number: 022 3260 (2003). These actions are in addition to those that the FTC has brought under the GLBA Safeguards Rule and/or the Consumer Information Disposal Rule. *See, e.g., U.S. v. PLS Financial Services, Inc., et al.*, Case No. 1:12-cv-08334, in the U.S. District Court for the Northern District of Illinois, Eastern Division (2012); *In the Matter of James B. Nutter & Company*, Matter Number: 0723108 (2009); *In the Matter of Premier Capital Lending*, Matter Number: 072 3004 (2008); *U.S. v. American United Mortgage Co.*, Civil Action No. 07C 7064, in the U.S. District Court for the Northern District of Illinois, Eastern Division (2007); *In the Matter of Nations Title Agency, Inc., et al.*, Matter Number: 052 3117 (2006).

Appendix B:

What Retailers Want You to Know
About Data Security¹

¹ Slides that follow are also available at: <http://www.slideshare.net/NationalRetailFederation/thingsto-know-datasecurity?ref=https://nrf.com/media/press-releases/retailers-reiterate-support-federal-data-breach-notification-standard>

What retailers want you to know about.....

DATA SECURITY

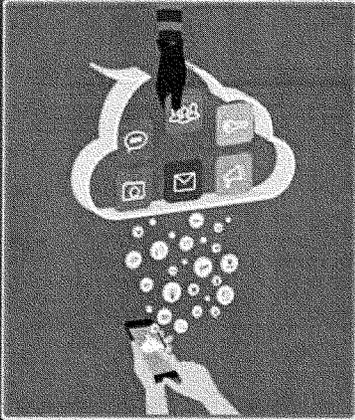


NRF RETAIL

BREAKDOWN

What is a data breach?

A data breach is the unauthorized acquisition of sensitive personal information in digital, electronic or computerized form that creates a risk of financial harm to a consumer.

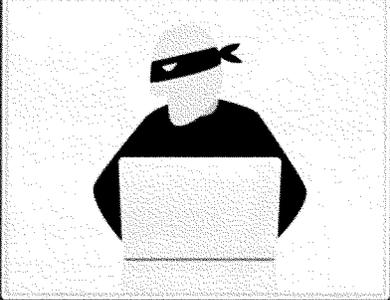


NRF RETAIL

ISSUE

Who is breaching?

Cybercriminals are constantly trolling for financial data in order to steal card numbers and convert them into cash.



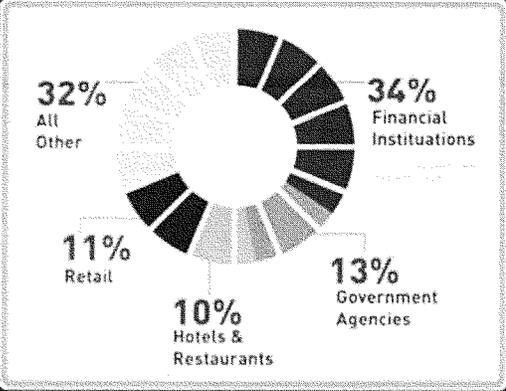
NRF RETAIL

ABOUT

Where do breaches happen?

Hackers don't discriminate – data breaches have targeted a wide variety of businesses from the entertainment industry to financial services.

According to Verizon, retail represents 11 percent of data breaches while the financial services industry accounts for 34 percent.



Industry	Percentage
Financial Institutions	34%
Government Agencies	13%
All Other	32%
Hotels & Restaurants	10%
Retail	11%

NRF RETAIL

ABOUT

Why retailers care about data security.

As a consumer-facing and reliant industry, retailers and merchants value every interaction with their customers.



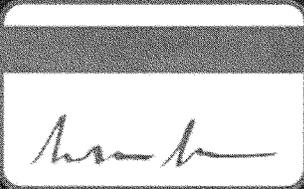
Retailers work every single day and make significant contributions and investments in data, information and payment security to ensure that the retail-customer relationship is secure and protected.

NRF RETAIL

PROBLEM

Cards are fraud prone

The thief creates a duplicate card, signs your name and makes a purchase.



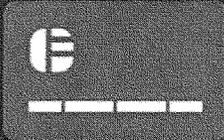
The thief uses your card, signs your name and makes a purchase.

NRF RETAIL

SOLUTION

PIN-and-Chip

Since 2005, the National Retail Federation has urged banks and payment card companies to switch to more secure PIN-and-chip cards, which replace the magnetic stripe with a computer microchip and replace the signature with a Personal Identification Number (PIN) to better protect consumers' financial data when they shop.



The new credit cards being issued this year need to have both a chip and a PIN, not just a chip as proposed by most banks and credit unions. The chip ensures that the card is the one issued by the bank but the PIN is needed to ensure that the person using the card is the actual cardholder and not a thief who stole your chip card.



NRF RETAIL

SOLUTION

PIN and CHIP

Only you know your PIN, so the thief can't enter it to complete an in-store transaction.

The thief cannot duplicate your chip card.

MAGNETIC STRIPE and SIGNATURE

The thief uses your card, signs your name, and makes a purchase.

The thief creates a duplicate card, signs your name, and makes a purchase.

YOUR CARD IS STOLEN

YOUR CARD INFO IS STOLEN

The safest cards deploy both PIN and Chip technology.

PIN and Chip is widely used around the world with great success; the United Kingdom saw a 75% drop in credit card fraud after implementation.*

American consumers deserve better.

NRF RETAIL

PROBLEM

Cyber-Threat Information Sharing

Congress must pass laws that make it easier for companies to share information and emerging threats without hesitation.



The illustration shows a government building on the left, a bank in the middle, and a shop on the right. A large double-headed arrow connects the bank and the shop, indicating bidirectional information sharing. The government building is also connected to the bank by a smaller arrow.

NRF RETAIL

SOLUTION

NRF's Efforts to Improve Threat Information Sharing

To help fight cybersecurity threats to retailers' systems, NRF created the Information Technology Security Council, which keeps retailers up-to-date on the latest news, information and threats. More than 150 retail companies are actively involved.



The illustration shows a government building on the left, a bank with a dollar sign in the middle, a shop on the right, and a server rack on the far right. A large double-headed arrow connects the bank and the shop, indicating bidirectional information sharing. The government building is also connected to the bank by a smaller arrow.

NRF RETAIL

PROBLEM

Notification isn't uniform

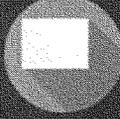
For the past decade, NRF has called for a uniform nationwide data breach notification standard that would preempt the patchwork of 47 state laws. This uniform federal law should be based on and reflect the strong consensus of state laws.

The current patchwork of state and local data breach notice laws with conflicting requirements doesn't work because it diverts limited resources that should be focused on restoring the integrity of a breached system.

NRF RETAIL

SOLUTION

Data Breach Notification Law

-  A nationwide breach notification law must preempt state and local laws so businesses and consumers understand what disclosures are expected regardless of when or where breaches occur.
-  Data breach notification should be appropriate, reasonable, relevant and timely.
-  Federal data breach notification requirements should be comprehensive and apply to every entity that maintains or transmits sensitive information, not just retailers.

NRF RETAIL

PROBLEM

Industries are held to different standards

Merchants have multiple tiers of data security standards. These include Payment Card Industry standards for all merchants accepting payment cards, as well as specific state standards to protect sensitive information. The Federal Trade Commission also enforces federal standards that require all merchants to have reasonable data security protections.

Other breached entities just need to follow industry-specific guidance.

NRF RETAIL

SOLUTION

Cover all entities involved in data breach

A data breach notification law should cover the entire payments system from card companies to telecommunications firms without exception or exemption. Arbitrary timeframes or industry-specific requirements that cover only certain entities should not be established.

Consumers need to know when financial data is breached.

PERCENTAGE OF BREACHES:

34%	Financial Institutions
32%	Mail Order
19%	Government Agencies
11%	Hotels
10%	Hotels & Restaurants

80% require that they notify
90% DOJ's NIS require that they notify

NRF RETAIL

Learn more: nrf.com/datasecurity

NRF NATIONAL
RETAIL
FEDERATION

