EXAMINING THE CURRENT DATA SECURITY AND BREACH NOTIFICATION REGULATORY REGIME

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

FEBRUARY 14, 2018

Printed for the use of the Committee on Financial Services

Serial No. 115–73

U.S. GOVERNMENT PUBLISHING OFFICE
31–346 PDF WASHINGTON : 2018

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MACARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

SHANNON MCGHAN, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

BLAINE LUETKEMEYER, Missouri, *Chairman*

KEITH J. ROTHFUS, Pennsylvania, *Vice Chairman*
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANDY BARR, Kentucky
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
MIA LOVE, Utah
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York

WM. LACY CLAY, Missouri, *Ranking Member*
CAROLYN B. MALONEY, New York
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
NYDIA M. VELÁZQUEZ, New York
AL GREEN, Texas
KEITH ELLISON, Minnesota
MICHAEL E. CAPUANO, Massachusetts
DENNY HECK, Washington
GWEN MOORE, Wisconsin
CHARLIE CRIST, Florida

CONTENTS

EXAMINING THE CURRENT DATA SECURITY AND BREACH NOTIFICATION REGULATORY REGIME

Wednesday, February 14, 2018

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

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

Present: Representatives Luetkemeyer, Rothfus, Lucas, Ross, Pittenger, Barr, Tipton, Williams, Love, Trott, Loudermilk, Kustoff, Tenney, Hensarling, Clay, Maloney, Scott, Green, Heck, and Crist.

Also present: Representative Waters.

Chairman LUETKEMEYER. The committee will come to order. Without objection, the Chair is authorized to declare a recess of the committee at any time. This hearing is entitled "Examining the Current Data Security and Breach Notification Regulatory Regime."

Before we begin, I would like to thank the witnesses for appearing before the subcommittee. We appreciate your participation and look forward to today's discussion.

And I recognize myself for 3 minutes for the purpose of delivering an opening statement.

Every year, the number and severity of data breaches seems to increase and more and more Americans seem to become victims of fraud and identity theft. Consumers are left not only facing financial harm, but also the daunting task of restoring the integrity of their personal information.

With constant technological advancements come more sophisticated threats to data security. Some of the largest financial institutions in the United States deal with hundreds if not thousands of cyberthreats on a daily basis.

Those attacks aren't just from one-off hackers but sometimes highly organized criminal enterprises backed by foreign nation-states. The majority of entities that handle personally identifiable information work hard to protect it from fraudulent acquisition and use.

As we consider reform of the current regulatory regime surrounding data security standards and notification requirements, we

should bear in mind that in many instances it is both the entity and the consumer that has been the victim of the crime.

While I recognize that companies work hard to guard against complex threats, it is sometimes the smallest and most avoidable errors that lead to the largest breaches. The company only has to be wrong once. The 2017 Equifax breach is a textbook example of the importance of good data security hygiene.

This is a vastly complex issue that impacts nearly every business in this Nation. But our primary focus throughout this endeavor should be the consumer. Can we create a system that puts them first? How can we safeguard their data without overburdening the entities that they patronize? When is the right time to notify them that a breach may have occurred?

Bottom line is that we, the American people, deserve better than the status quo. All entities that handle our personal information have some responsibility to maintain data security standards that protect our information and to keep us better informed of instances that could lead to theft, fraud, or economic loss. We have the right to this information so we can be empowered to protect ourselves.

Today's hearing will provide the committee with an opportunity to hear from witnesses with diverse professional backgrounds and opinions on data security. I want to thank them for offering their perspectives today. I look forward to your testimony and to continued collaboration on this incredibly important issue.

The Chair now recognizes the Ranking Member of the subcommittee, another gentleman from Missouri, Mr. Clay, for 5 minutes for an opening statement.

Mr. CLAY. Thank you, Mr. Chair. At this time I will forego the opening statement and hopefully we can get to the witnesses. I yield back.

Chairman LUETKEMEYER. Mr. Rothfus?

Mr. ROTHFUS. No.

Chairman LUETKEMEYER. We are done with opening statements. You guys are lucky this morning.

With that, we welcome testimony of our witnesses, a number of you have names that are Luetkemeyer, a little difficult to pronounce, and I apologize if I get them wrong this morning.

But Mr. Aaron Cooper, Vice President for Global Policy, BSA - The Software Alliance; Ms. Kim Sponem, President and CEO of Summit Credit Union on behalf of the Credit Union National Association; Mr. Nathan Taylor, Partner, Morrison & Foerster, LLP; Professor Mack Rotenberg—is that right, or Rotenberg?

Mr. ROTENBERG. Marc. Marc Rotenberg.

Chairman LUETKEMEYER. Marc. Marc Rotenberg, President, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center; and Mr. Paul Rosenzweig—pretty close?

Mr. ROSENZWEIG. Much better than most, sir.

Chairman LUETKEMEYER. OK. Obviously we are not right yet, that is the problem. But that is OK—appreciate your diligence—Senior Fellow, R Street Institute.

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

Just a little tutorial on the lighting system in front of you. Green means go. When you see a yellow one pop up there that means you have 1 minute to wrap up, and red means stop. I have a gavel up here that we will make that emphatically known if we need to.

I would ask that you pull the microphones close to you. They do move. They are not stationary on the desk there. You can pull them toward you so we can hear you. Sometimes if you speak softly it is a little difficult in this large room to get the right acoustics.

So with that, Mr. Cooper, you are recognized for 5 minutes.

STATEMENT OF AARON COOPER

Mr. COOPER. Thank you, Mr. Chairman. Good morning Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee. My name is Aaron Cooper and I am Vice President for Global Policy at BSA - The Software Alliance.

BSA is the leading advocate for the global software industry in the United States and around the world. Our members are at the forefront of cutting edge, cloud-enabled data services that have a significant impact on U.S. job creation and the global economy.

Data security is crucial to our members and to their customers in every industry sector. I commend the subcommittee for holding this hearing on such an important topic, and I thank you for the opportunity to testify.

BSA's support for data security and breach notification legislation dates back more than a decade. Persistent, high-profile security incidents make the need for thoughtful legislation more important now than ever.

Our economy today and economic growth and job creation in the foreseeable future is rooted in digital data. Every industry today is improved through the use of software to store, transfer, and analyze data.

But the embrace of the digital economy cannot be taken for granted. If customers do not trust that their data will be kept secure, they will not use the technology. Our companies compete on privacy and security. Their customers rightfully demand it.

Data breaches erode that trust in digital services and can have a significant cost on the economy.

The security threats we face today are global, the adversaries increasingly sophisticated, and the motivations are far more complicated than in the past. Malicious actors use both internal and external threats to commit financially motivated crimes and other forms of espionage.

In some cases, advanced persistent threats are conducted by well-resourced teams of specialists that are often linked to nation-state actors. Organizations that hold sensitive data need to incorporate high standards of risk management.

This does not always require adopting excessively costly or cumbersome security measures. In fact, reasonable diligence can make a considerable dent in the problem. Experts suggest that more than 90 percent of data breaches could be preventable through basic cyber hygiene.

Compromised or weak user credentials account for the vast majority of hacking-related breaches and patched software could prevent nearly 80 percent of security incidents.

BSA is committed to being part of the solution and, along with our members, is leading on several important efforts. First, BSA recently released a new cybersecurity policy agenda which addresses the need to promote a secure software ecosystem, develop a 21st-century cyber workforce, and embrace emerging technologies.

Second, BSA members have been leading advocates of security by design principles and secure development lifecycle approaches to developing software.

Third, the industry has developed and deployed layered defenses from protection at the data and document level to the network and perimeter level.

Fourth, use of cloud-based services offer an important option for data security. Just as a bank can better protect individual financial assets of its patrons, cloud service providers can provide a level of protection for their customers' digital assets beyond what many small and medium-sized businesses can do on their own.

It is important to remember that even when customer data is placed in a cloud infrastructure, security remains a shared responsibility. Cloud providers can help reduce the operational burden associated with securing data, but security is a process, not an end state.

The cloud provider and customer both have responsibilities for managing the security of data.

While the industry is taking important steps, only Congress can ensure that there is a uniform and effective Federal standard. In BSA's view, legislation should aim to achieve three goals.

First, legislation should minimize the risk of data breaches. It should require companies that collect or maintain sensitive personal information to implement reasonable data security practices. The practices should be scoped in size to the complexity, sensitivity, and volume of personal information on a company's systems.

Second, legislation should mitigate the impact of breaches that do occur. Legislation should ensure that consumers receive timely and meaningful notification based on a risk-based analysis.

Third, legislation should create uniformity. We currently have a thicket of 48 different State data breach notification standards. The variation between the State laws are not trivial and it is unhelpful in the wake of a breach of personal information to have a company working with a team of lawyers to understand what requirements must be met in each jurisdiction before notifying customers of the breach.

In conclusion, there is a lot that Congress can do to improve the situation for both businesses and consumers. Well-crafted legislation can facilitate rapid and robust responses to significant security incidents. And Federal guidance on data security will drive stronger security measures across the Internet ecosystem.

BSA strongly supports these goals, and we look forward to working with the subcommittee to achieve them. Thank you, and I look forward to your questions.

[The prepared statement of Mr. Cooper can be found on page 40 of the Appendix]

Chairman LUETKEMEYER. Thank you, Mr. Cooper.

Ms. Sponem, recognized for 5 minutes. Please turn your microphone on and pull it close. Thank you.

STATEMENT OF KIM SPONEM

Ms. SPONEM. Thanks. Chairman Luetkemeyer, Ranking Member Clay, members of the subcommittee, thank you for the opportunity to testify on this extremely important topic. My name is Kim Sponem and I am Chief Executive Officer and President at Summit Credit Union testifying on behalf of the Credit Union National Association.

Summit Credit Union, headquartered in Madison, Wisconsin, is a State-chartered credit union founded in 1935. We have $3 billion in assets and serve 175,000 members, which is quite small compared to regional and national banks.

Like all credit unions, we are a not-for-profit institution, owned by the very members we serve. Summit Credit Union offers a full array of financial services to meet the needs of our members, including debit and credit cards.

Unfortunately, data breaches occur far too often. Consumers and financial institutions are harmed by data breaches when entities and organizations, including merchants, fail to take necessary steps to protect consumer data.

Community financial institutions foot the bill when companies fail to secure customer information when many do not need to store that information in the first place. Breaches cost Summit Credit Union over $1 million in 2017 alone, but more importantly, the negative impact on consumers is significant and sometimes devastating.

Imagine you are making a purchase and your card is declined. You don't know why. There is a line behind you. You are embarrassed and concerned. You figure out a different way to pay or you walk away angry.

You call your financial institution. There are fraudulent charges on your card. You now know why the purchase was declined because of fraud, but now you have the stress of wondering just what information did the fraudsters gain on you?

Or are you using your debit card in another country to get currency? It is shut down. Now what do you do? You are worried someone is depleting your checking account. How long will it take to get that resolved? How will you get your money in another country? Panic sets in.

Even worse, someone stole your identity and took out a loan in your name now your credit is compromised. How do you get it back? It can take years and tens of thousands of dollars to rectify.

Meanwhile, my credit union is working hard to get you another card at $3 to $5 per card, overnighting them when needed at our expense. We work with you to address the fraudulent charges that are on your card that we pay for.

We look to increase our fraud monitoring systems that are expensive and labor-intensive. And most of all, we spend the much-needed time with our members to help them navigate the financial system.

Once you have new cards then remembering to update your automatic payments is the next step. If you forget, you now are delinquent with that company.

All fraud and fraud mediation is paid for by financial institutions. There is no incentive for companies that hold personal information to protect it. And that is just plain wrong.

Under current law, credit unions and banks are subject to data security requirements, necessitating the development of procedures and systems to protect consumer information from theft, including notifying consumers in the event of a data breach.

However, other entities that hold personal information are subject to no such standards. Any company that holds consumers' personal information necessarily or unnecessarily should be held to a national standard. Americans deserve a strong national data security standard that requires all businesses to protect and safeguard personal information.

Companies that do not need to store personal information should either not store it or be subject to the standard. Companies should not be allowed to put consumers at undue risk.

And communicating a data breach in a timely manner allows consumers and financial institutions the ability to try to reduce possible losses with early detection and awareness.

The current system is not fair or sustainable. Consumers are protected from losses because financial institutions bear the responsibility for reimbursing them. Those that are negligent should bear the cost.

Protecting data is expensive and it is labor-intensive. But a company that stores information needs to invest in these protections for consumers as a cost of doing business, or not store the information at all.

In summary, it is our hope that this committee makes data security one of its top priorities in 2018. We ask that any legislation proposed would include these three priorities: One, a standard for all companies holding personal information; two, a requirement to communicate breaches in a timely manner; and three, a responsibility for negligent companies to bear the costs.

We will work with you to protect consumer data and increase accountability. Companies may not want to invest in protecting data, but it is a matter of responsibility and duty that goes with holding that information.

On behalf of Summit Credit Union and the National Association I would like to thank you for this opportunity to share my views. And I would be happy to answer any questions. Thank you.

[The prepared statement of Ms. Sponem can be found on page 72 of the Appendix]

Chairman LUETKEMEYER. Thank you, Ms. Sponem.

Mr. Taylor is recognized for 5 minutes.

STATEMENT OF NATHAN TAYLOR

Mr. TAYLOR. Mr. Chairman, Ranking Member Clay, and members of the subcommittee, my name is Nathan Taylor and I am a partner at the law firm of Morrison & Foerster. My practice is focused on helping financial institutions and other companies protect the security of their sensitive information and respond to security incidents that unfortunately but inevitably occur.

My colleagues and I have represented companies in responding to a number of the largest and highest profile data breaches in American history.

I am pleased to be here today to provide you with background on the State safeguards laws and the State security breach notification laws. At the outset, however, I want to stress that I share your concern about the critical need to protect American consumers and American businesses from the increasingly sophisticated cybersecurity threats that we face today.

Cybersecurity impacts not only the security of our own sensitive personal information, but in the Internet-connected world in which we live, it impacts our very way of life.

In my view, we need a national standard to address what is truly a national issue, and I also believe that a national standard would ultimately be good for both the American consumer and American businesses.

For more than a decade I have tracked the State laws as they have developed in this area. When you review the current landscape of State laws, you find a complex matrix of inconsistent, sometimes duplicative and often contradictory requirements.

With respect to State safeguards laws specifically, today only 15 States have laws in effect that impose general requirements on all companies to protect the security of sensitive personal information. Most of these safeguards laws impose only a high level obligation to take reasonable steps to protect sensitive information.

Only a few include detailed security requirements, and those are often modeled on the Safeguards Rule issued by the Federal Trade Commission pursuant to the Gramm-Leach-Bliley Act (GLBA).

In contrast, however, today, 35 States do not have generally applicable laws that require all companies to protect sensitive personal information.

If you are an American, where you live should not impact whether there is a legal obligation to protect sensitive information about you. In my view, this point is not controversial. We need a national standard for security to ensure that all Americans are protected while also leveling the playing field for American businesses.

With respect to breach notification, 48 States, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted breach notification laws. Although these laws ostensibly share the same purpose, they are far from uniform and vary significantly in terms of their requirements.

For any given breach the many differences among the laws impacts whether at all a consumer receives a breach notice, what that notice says, when it is sent, and even how it is sent. In addition, the inconsistencies among these laws complicate the process for companies in providing notice to consumers.

Even for companies who respond to an incident diligently, investigating a breach, restoring the security of systems, and providing notice to consumers takes time. It is a complex process that is made more difficult by the need to comply with 52 different breach laws. A single nationwide standard for breach notification would address this issue.

In closing, I note that Congress, including this committee, has considered the issue of data security for 15 years. In my view, the

time for Congress to act is now. In considering legislation I would recommend that this committee be guided by four principles.

First, a Federal bill should include strong yet flexible and scalable data protection standards for all companies.

Second, a Federal bill should require notice to consumers of breaches that put them at risk of harm.

Third, a Federal bill should include a safe harbor for compliance with the existing Federal data security standards.

And finally, a Federal bill should pre-empt State laws to ensure that all Americans receive the same level of protection regardless of where they live.

Thank you for the opportunity to speak with you today, and I am happy to answer any questions that you might have.

[The prepared statement of Mr. Taylor can be found on page 83 of the Appendix]

Chairman LUETKEMEYER. Thank you, Mr. Taylor.

Professor Rotenberg, recognized for 5 minutes.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Mr. Chairman, Ranking Member Clay, and members of the committee, thank you for the opportunity to speak with you today. My name is Marc Rotenberg. I am President of the Electronic Privacy Information Center.

We are a nonpartisan research organization established in 1994 to focus public attention on emerging privacy issues. I have also taught privacy law at Georgetown for more than 25 years and am the author of several books on privacy law.

I have provided for the committee a detailed statement that I ask be entered into the hearing record. I would be happy to briefly summarize my comments, if that is OK? Thank you.

Let me say at the outset that data breaches today pose an enormous challenge, not only to American families but also to our country. Previously, consumer privacy laws were enacted to safeguard consumers against the misuse of their personal data.

But what we are increasingly aware of is that foreign adversaries are targeting the personal data stored by American firms here in the United States. And you see as a consequence when companies engage in lax security practices, they put their clients and their customers at risk, not only of the misuse of the data but also of identity theft and financial fraud from foreign actors.

A related concern that I would like to bring to your attention is the growing divergence between U.S. privacy laws and privacy laws in Europe. As you may be aware, the European Union is moving in May of this year to establish a comprehensive approach to privacy protection known as the General Data Protection Regulation.

That law is already having a big impact and I would say a positive impact on the practices of U.S. firms operating in Europe. But the increasingly critical question is whether the United States will update its privacy laws to address growing concerns about the protection of personal data held in the U.S., not only on U.S. consumers but also on the consumers in countries where we do business.

So for both of these reasons, I think there is an enormous urgency in this committee moving forward for strong proposals for

privacy protection. And I have outlined in my testimony several key principles that I hope you will consider, as well as brief comments on some of the bills that are pending in this committee and elsewhere in Congress.

I want to comment on a few of the points that were made earlier and highlighting also statements that are in my prepared testimony. I think the key point is that you want to establish a Federal standard but it should be a Federal baseline standard.

And this is the traditional approach to privacy protection in the United States. If you go back to the Video Privacy Protection Act or the wiretap statute or other consumer privacy laws, the approach to privacy protection has been one that recognizes, as the other witnesses have said, the need to ensure a Federal standard that provides baseline protection but also allows the States to regulate upwards and to respond to emerging privacy threats as they emerge.

Just looking at the field of data breach notification and the experience in the State of California, what you will see is that as the State confronted new forms of data breach, first it was financial fraud and then it was medical records, the State was updating its laws to address the new challenges and to provide new and necessary coverage to ensure that consumers would be aware of the new types of data breach.

This is entirely consistent with our Federalist form of Government that leaves to the States the authority to establish stronger privacy protections when necessary. So I would certainly agree with the other witnesses on the need for a national standard, but I would urge that that be a baseline standard.

Some of the other key points in my testimony include the need for prompt breach notification. It simply takes too long today to tell people that their personal data has been compromised.

In the credit reporting industry we think it is important to establish across the board data freezes so that consumers can make the determination affirmatively when to disclose their personal data to others rather than to have to wait until the breach occurs and then to take additional steps to safeguard personal data that has already been compromised.

I would be pleased to address other points in my testimony, and thank you again for the opportunity to speak with you today.

[The prepared statement of Mr. Rotenberg can be found on page 57 of the Appendix]

Chairman LUETKEMEYER. Thank you, Professor.

Mr. Rosenzweig, recognized for 5 minutes.

STATEMENT OF PAUL ROSENZWEIG

Mr. ROSENZWEIG. Thank you, Mr. Chairman, Ranking Member Clay, members of the committee. I thank you for the invitation to join you today. My name is Paul Rosenzweig. I am a Senior Fellow at the R Street Institute. We characterize ourselves as a pragmatic think tank, which I guess means that we think the free markets work except when they don't.

There is good evidence that the free markets do not fully work in the cybersecurity arena and that the market does not adequately price in the costs of cybersecurity.

Recent history is, of course, replete with examples of data breaches like the Equifax breach and the harm they have caused. I myself have been the subject of at least three breaches in the last couple of years, Equifax, Home Depot, and the OPM breach.

And as the Verizon data breach annual report reflects, in 2016, the last year for which we have some data, more than 40,000 incidents and 2,000 confirmed breaches have occurred.

So make no mistake. Cyberthreats are real and recent experience has shown that neither the private nor the public sector are fully equipped to cope with them.

Given these threats, we should expect that the market would provide a solution. Why is that not enough? The answer I think lies in the conception of externalities, that is, the fact that activity between two economic actors may directly or unintentionally affect a third party.

Cybersecurity has those types of negative externalities. The most important one is what we call a pricing problem. That is that private sector actors often do not internalize the costs of security failures in a way that leads them to take adequate protective steps. When software fails to prevent an intrusion or a service provider fails to interdict a malware attack, the costs are borne entirely by the end users.

In this way, security for the broader Internet is a classic market externality. How then should Government respond to this problem?

First and most importantly we should guard against what public choice theory calls rent-seeking. That is the idea that we should not foster the right result but rather the result that concerted lobbying efforts favor.

Second, we must be careful of inflexible float to change mandates. The Government's hierarchical decisionmaking structure allows only slow progress in adapting to this phenomenon and operates far too slowly to catch up with the pace of cyber change, if you will.

We make decisions at the speed of conversation. But change happens at the speed of light. Of course, whenever we have chosen to address a pricing problem through litigation there are also significant costs, most notably transaction costs. Operating the civil justice system is expensive and participating in that system even more so.

Those costs which are unrelated to the merits of the failure or the litigation have a strong tendency to distort the market in ways that are often unanticipated.

So then what is the right approach? My counsel to you would be first do no harm. In the end, if a regulatory approach is chosen at all, it should be flexible and scalable too and a standard-setting approach with a light administrative enforcement mechanism rather than a hard mandatory approach with a heavy civil sanction.

Most importantly, we must develop a system that creates more certainty than it does uncertainty, and that requires two things: Guidance and reassurance. As to guidance, we need a model that relies on a flexible standard but also one that is clearly articulated.

By contrast, for example, today much of the guidance from the FTC (Federal Trade Commission) to consumer enterprises on acceptable cybersecurity practices comes in the form of consent de-

crees that, taken together, articulate a very indefinite standard of reasonable behavior. That is a poor way to set standards.

Second, no enterprise will invest resources in achieving standards without some assurance that doing so will benefit the enterprise. In reality, a major portion of that benefit will lie in the fiscal security of knowing that the enterprise has taken adequate steps to avoid liability. So we need either an implicit or an explicit form of safe harbor that encourages people to adopt the standards we develop.

So what should our standard-setting system look like? Well, we have a good example in the NIST (National Institute of Standards and Technology) framework, a collaborative bottom-up approach that collects best practices and advocates for them as the best standard available.

If we follow these precepts, if we focus on standard setting rather than rulemaking and guidelines rather than mandates, will go a long way toward advancing cybersecurity and ameliorating the failures in the marketplace.

I should caution that no solution we can devise will be perfect. This is truly an insoluble problem that cannot be eliminated altogether. But there are in fact better or worse answers, and I commend the subcommittee for its attention to the problem. And I look forward to answering your questions.

[The prepared statement of Mr. Rosenzweig can be found on page 49 of the Appendix]

Chairman LUETKEMEYER. Thank you, Mr. Rosenzweig, appreciate your comments this morning. Although they were honest, you just said we couldn't solve the problem, so at least we can talk about it, huh? The Congress is really good at that. We can talk a lot, can't we?

With that, I will recognize myself for 5 minutes and begin the questioning. Again, thank all of you for your comments. As many of you indicated we have almost daily breaches now, and the American public is clamoring for some sort of solution to some of these problems.

And we are trying to put together a bill that hopefully will address some of the concerns and take into account some of the suggestions that you have given us this morning. And we certainly appreciate your input.

Let me start out with Mr. Rosenzweig with regards to one of the issues I think that is key to this whole situation is the pre-emption of State law, all of you mentioned this very thing.

To me it looks like we have two choices. One you pre-empt State law and be able to protect the consumer data. Or the other is you allow the hodgepodge of laws to continue and the consumers beware. Where would you come down on this?

Mr. ROSENZWEIG. Well, rather than characterizing them as a hodgepodge, I would say that federalism and competition is one of the ways that a market can function. The other way is to impose uniformity across the entire Nation. That has the economic advantage of eliminating redundancies and conflicts and reducing costs.

What I would say is the worst answer or the worst of both possible worlds is to partially pre-empt State law, to set a baseline standard that does away with federalism in the first instance but

doesn't eliminate the uncertainty of multiplicitous laws in the second instance. You don't gain any of the benefit and you cost a lot—

Chairman LUETKEMEYER. Would you believe we had an across-the-board exemption that allowed for a Federal standard that would provide a better safeguard for data for people, though?

Mr. ROSENZWEIG. I think as an economic matter, if you are going to—

Chairman LUETKEMEYER. I am not talking about economics. I am talking about the ability of people to protect their data.

Mr. ROSENZWEIG. There would be more consistency and therefore more likelihood of full compliance. The inconsistency of the rules is part of what generates some of the uncertainty. So yes, sir.

Chairman LUETKEMEYER. OK, thank you. You make a good attorney. Let me go with the question with regards to notification. I know everybody has a different idea of this. You talk to the companies they want, and we have seen examples of this, anywhere from 2 weeks to 1 year before people were notified.

The American public deserved better than that, and because of those, in my mind, lousy ways of trying to work and manage their breach, they have lost the trust of the American people. So I don't know how we can get it back unless you go to a zero, immediate notification.

This is what we need to go to, and I think the American public is going to clamor for this, and my thought process is that while the breach is going on you know what is going on and you are ascertaining exactly how much information and what information was lost, whose information was compromised.

You can already know, OK, we have a breach. Now we have to start setting up some sort of a notification process.

And I think you can do two tracks on this so that whenever you finally do realize that you have a compromise situation where you have to be notifying people, you can do that on an immediate basis. Anybody like to comment on that, see where you are on that?

Mr. ROTENBERG. Well Mr. Chairman, I agree with you. I think, in fact, our recent experience with Equifax demonstrates the need for prompt breach notification. The company was aware in March 2017 that they had a problem with a key security protocol that they failed to update.

Yet it wasn't until August, 4 months later, that they actually took steps to begin to notify the public of the potential that their data had been breached.

And of course as long as that software was not updated the breach was ongoing. So the breach is necessary not only to provide information to consumers so that they can act, but also to ensure that the company is being diligent when it uncovers a problem.

Chairman LUETKEMEYER. Very good. Anybody else like to comment on that?

Ms. Sponem?

Ms. SPONEM. We had a situation in Madison where there was a local processor that processed credit cards for various restaurants. And they had been breached and did not notify anyone. It took them weeks and into over a month to start to work on the patches that they needed to do in order to shut that down.

So meanwhile, the hacker, every single time someone used their credit card at one of those restaurants, they were just getting new credit card information. We had customers who had to get their credit card reissued four times during that period.

Chairman LUETKEMEYER. I would like to make one quick comment. I know that yesterday in the National Journal there was an article with regards to Europe beginning to come on, and I think Professor you made this comment with regards to new data rules coming out.

In their data rules they are looking at a 72-hour window within which to disclose this, although it doesn't say in here whether you actually ascertain exactly the kind of information that has been breached and you know that there is actually some people's information had been compromised. I think that is a key component of this.

But just a quick, would everybody agree that immediate notification has to be there or some other timeframe?

Mr. Cooper? I am running out of time.

Mr. COOPER. Mr. Chairman, I think it is really important that there be prompt notification, and I think that the response from companies needs to be strong and immediate. But we also need to look at what is going to be best for consumers.

And one of the concerns about having an artificial deadline about when notification has to happen is that the initial information is not always the accurate information. And it is more important that the information be accurate than that it be fast.

Chairman LUETKEMEYER. Very good.

Mr. COOPER. And I think that with the FTC and State attorneys general being able to make that determination—

Chairman LUETKEMEYER. Very good. My time is up. I have to set a good example here. You will all be able to come to—hopefully my guys have been listening over here and we are going to get some good questions on this, because this is a key component to be able to go forward here.

With that, Mr. Clay from Missouri is recognized for—the Ranking Member is recognized for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

And Professor Rotenberg, you have written previously that without comprehensive legislation the data breach problem will only get worse. As part of such legislation, what type of personal information should be explicitly covered?

Mr. ROTENBERG. Mr. Clay, this is a critical question, not only because personal data such as home address and Social Security number and financial records and educational records are readily understood as personal data, but also increasingly in an era of Big Data we have a lot of information that is deidentified but can be reconstructed as personal data.

So when we talk about personal data in the 21st century, we need to understand that it is information that appears as personal data and is familiar or could be made personally identifiable. So as a starting point for privacy legislation, we think it is important that there be a broad scope and that this particular problem be well-understood.

Mr. CLAY. And should a harm threshold be used to trigger notification of a breach or should all breaches be disclosed?

Mr. ROTENBERG. Well, this is a critical question. The problem with a harm threshold is that it is oftentimes left to the company to make a determination about whether they think the consumer has been harmed. And in our view the better approach says to the company if a breach has occurred, notify the consumer and then let the consumer determine the scope of the harm.

Oftentimes companies don't have the full picture of what the consequence will be if customer data is breached. And that is why we think that the harm standard is too high. It results in too little notification.

Mr. CLAY. Thank you for that. In your testimony you mentioned that credit rating agencies should have an automatic credit freeze. Could you expound on that and tell me how would a consumer unfreeze that credit then?

Mr. ROTENBERG. Right. Well, I think this is just common sense. As we also say, the credit reporting industry is vital to the American economy and consumers need the ability to obtain credit, to get a home loan or purchase a car. We all understand that.

But when the consumer is making one of those big life decisions the person should be able to say OK. Now I want this company to have access to my credit report. So it becomes an affirmative decision.

The problem with the current system is that companies routinely get access to personal data, whether or not the customer has any intent of doing business with the company. And this also contributes to identify theft.

So if we change the default, give consumers the ability to disclose the customer report, the credit report, prior to the purchase, we think that would be good for the customer. It would be good for the merchant and would reduce the levels of identity theft.

Mr. CLAY. Would that have had an impact on the Equifax?

Mr. ROTENBERG. Absolutely. The problem with Equifax is the data became widely available and consumers were asked after the fact to race around and put credit freezes in place. And at that point it is too late.

Mr. CLAY. Yes, yes. And in recent testimony before the Senate you underscored the implications that the massive Equifax breach has for U.S. trade relations, citing the fact that more than 15 million U.K. customers were impacted and the fact that the data exposed by the breach is, as you put it, "a gold mine for identity thieves." Can you expand on that concern?

Mr. ROTENBERG. Well, this is the point that I raised in my opening statement. Traditionally when we talked about privacy law in Congress the focus was the impact on U.S. consumers. But of course now we live in a global, Internet-connected environment.

Many U.S. companies are doing business overseas, and those governments are looking at U.S. privacy law and trying to assess if we have adequate privacy protection for the records of their citizens.

So when the Equifax breach occurred, it didn't just impact American consumers. It impacted people in the U.K. and Canada and elsewhere around the world. I think it is very much in the long

term interest of the U.S. economy to strengthen our privacy laws because other countries are becoming increasingly concerned about the weak privacy standards we have.

Mr. CLAY. And you had mentioned that the E.U. was moving forward—

Mr. ROTENBERG. Yes, that is correct.

Mr. CLAY. —with an initiative and we should probably look at that also and take some of the good points of it I guess?

Mr. ROTENBERG. Thank you.

Mr. CLAY. Thank you.

I yield back.

Chairman LUETKEMEYER. The gentleman yields back.

With that, we go to the gentleman from Pennsylvania, the Vice Chairman of this committee, Mr. Rothfus, recognized for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Ms. Sponem, in your testimony you discussed how merchants and other companies that are not banks or credit unions are a source of vulnerability and cost.

You wrote the following, "Financial institutions like Summit Credit Union foot the bill for the fallout and subsequent fraud that comes from the breach of personal information from merchants and other companies' failure to adequately protect and secure customer information. "

In your experience, are merchants and other non-financial companies a major avenue for data breaches?

Ms. SPONEM. Yes, I believe that they are a major avenue for breaches. I believe that most breaches do come from those sources.

Mr. ROTHFUS. And can you quantify again how much these breaches cost your credit union annually?

Ms. SPONEM. So in 2017 we spent over $1 million on breaches. And that has increased year-over-year. So in 2013 it was around $350,000. It increased 20 percent in 2014, and today it is over $1 million.

Mr. ROTHFUS. Mr. Taylor, while I agree that cybersecurity and breach prevention and notification should be national concerns, I also acknowledge that small businesses may post less risk and have fewer resources available to address potential risks.

What is the best way to tailor data security and breach notification requirements to the characteristics of businesses that vary in size and capacity?

Mr. TAYLOR. It is a great question, and I think the key is that you have a flexible and scalable standard. And that is something that a number of us on the panel have highlighted today.

You need a standard that takes into account the size, complexity, and scope of the business' operations so the standard can apply to the smallest company in America to the largest.

I think it is critical that everyone has at least some obligation but then the amount of resources that you have and the size of your organization should dictate the extent of the expectations.

Mr. ROTHFUS. Do you know what NIST's role is in setting cybersecurity standards?

Mr. TAYLOR. The NIST issued the cybersecurity framework pursuant to an Executive Order.

Mr. ROTHFUS. Are entities required to use the NIST framework?

Mr. TAYLOR. No.

Mr. ROTHFUS. What Federal agencies should enforce the law and determine what compliance with the law in this area would look like? Any opinion there?

Mr. TAYLOR. Yes, absolutely. I think you have to recognize a couple points here. First, we do have existing standards under the Gramm-Leach-Bliley Act and under HIPAA (Health Insurance Portability and Accountability Act). And I think for those areas you should continue to follow the prudential regulation model.

For example, the financial regulators enforce over the financial institutions. And then I think that when you are looking for who else should enforce, I think you have to start with the Federal Trade Commission, who has historically played a very active and strong role in this space.

Mr. ROTHFUS. Mr. Cooper, if I can ask you, we all recognize that Congress does not want to create a situation whereby breached entities are forced to inundate consumers with insignificant notifications to the point that the breached entity is notifying wolf.

With that in mind, where should the responsibility and authority reside in determining a direct risk threshold of identity theft that would trigger a notification?

Mr. COOPER. Well, I think, again, we need to look at it from the perspective of what is going to be helpful for the consumer in responding to a breach that might have an effect on them. I think they are most likely going to be responsive to the entity that they know has their data.

So in Ms. Sponem's example, for instance, the restaurant that a customer went to where their credit card was used, making sure that entity is communicating with the customer I think is crucial with some actionable information so that it is not just a notice that there has been a breach but here are things that you can do.

Mr. ROTHFUS. Mr. Taylor, if I could go back to you? In your testimony you described the current patchwork of State notification laws as a, quote, "complex matrix of inconsistent and sometimes duplicative and often contradictory requirements."

Clearly, there is a case to be made that a national standard would be more appropriate and that it would significantly reduce the compliance burden for firms.

If we were to establish a national breach notification standard, what information would need to be included? What do consumers need to know if their information has been improperly accessed or stolen?

Mr. TAYLOR. I think there are a few key points that you should focus on. First, a description of the incident, what happened. What information was involved? What is the company doing about it? And steps that the consumer could take to protect herself from harm.

Mr. ROTHFUS. I yield back. Thank you.

Chairman LUETKEMEYER. The gentleman's time has expired.

Then we go to the Ranking Member of the full committee, Ms. Waters, from California, recognized for 5 minutes. Welcome.

Ms. WATERS. Thank you, Mr. Luetkemeyer. I have an opening statement that I will submit for the record, and I appreciate you holding this hearing.

Mr. Rotenberg, Chairman Hensarling has said that in light of the Equifax breach it should be obvious to all that our committee will revisit the Data Security Act, legislation that our committee took up nearly 2 years ago.

The law included sweeping language that would have pre-empted State law, in which the Massachusetts attorney general at a minority day hearing that Democrats called, indicated would drastically undercut Massachusetts data security regulations.

The New York attorney general's office agreed with this perspective in their testimony before our committee. So in your view, if the choice is between the status quo or Federal legislation that pre-empts States' ability to take action to protect consumers and bolster data security requirements, which option would you prefer?

Mr. ROTENBERG. Thank you, Congresswoman, for the question. I am somewhat familiar with the Data Security Act, the 2015 bill, and I am also aware of the objection of many State officials and consumer groups.

I think it would be better not to pre-empt State laws that currently provide strong protections to consumers. I think there is a very real risk, in fact, that if you pass a national standard that is weaker than what many of the States currently provide, you will see an increase in the levels of identity theft and financial fraud in the United States.

Because it is actually those State officials and the State attorneys general on the front lines of this problem who are dealing with State residents and businesses trying to come up with the best legislative solutions.

So the practical consequence of capping that effort would be to remove the most well-informed, the most effective, and the most responsive policymakers from this field. I think it would be a terrible mistake.

Now, I do think Congress has a role to play and has always played an important role establishing a baseline standard when it becomes aware of an emerging privacy issue. And most certainly the protection of personal data is an emerging issue.

But I have no difficulty saying quite simply, a measure that would pre-empt State law would leave many more American consumers at risk of identity theft and financial fraud.

Ms. WATERS. Thank you. And in some discussions that I have had with some members here, they have said that this area that we are dealing with cybersecurity issues, that you need flexibility and you need to be able to continue to strengthen your efforts to ensure that you have the kind of protections that are necessary.

And that means that the States may be able to move faster, may be able to initiate changes, upgrade, do all kinds of things that perhaps the Congress of the United States could not easily and readily do. Is that a concern?

Mr. ROTENBERG. Well, I think that is the actual experience in this field. I think there are some fields where there is no question that Congress does need to establish a comprehensive national standard.

But I think there are other fields, and privacy is most certainly one, where the nature of the subject matter and the expertise that

exists at the States underscores the need for our Federalist approach to coming up with innovative solutions.

It was actually Justice Brandeis, known for his famous opinion on the right to privacy, who also described the States as the laboratories of democracy. And we see that in the protection of privacy. This is where the innovative legislation comes from.

Ms. WATERS. Well, my concern is that when you start to talk about national standards and you are dealing with all of these Members of Congress who come from different States and you have to basically come up with an agreement, a consensus dealing with all of the concerns, that the national standard is usually a race to the bottom almost.

And that it does not recognize that some States, such as have been identified as New York and Massachusetts, have good standards, higher standards. And a national standard would certainly not match that which some States already have and could have.

So I thank you for being here today. I appreciate your testimony. And I think that we should take into consideration what you have said because pre-emption of State laws is a serious effort that should be taken seriously and not done in the interests of just trying to have something.

I yield back the balance of my time.

Chairman LUETKEMEYER. The gentlelady's time has expired.

With that, we go to the gentleman from North Carolina, Mr. Pittenger. You are recognized for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman. Thank you for leading this very important hearing and would like to again thank all of our witnesses for being with us today. Your input is so critical for each of us on this committee.

Clearly, data and cybersecurity need to be at the forefront of the agenda for the U.S. Congress. Over the last several years we have had big and small companies that have been affected by related security breaches. And obviously the Equifax is at the forefront of an issue that we have all sought to consider and evaluate where we go forward.

I would like to ask at this point, Ms. Sponem, what is the nature of the FTC's oversight of the credit bureaus' data security operations? Would you expand on that some more?

Ms. SPONEM. What is the oversight of the FTC with regard to this issue?

Mr. PITTENGER. To the credit bureaus' data security operations.

Ms. SPONEM. So we fall under the GLBA standards, and we believe that we are required to follow those. And we believe that they should as well.

Mr. PITTENGER. Sure. How does the FTC's oversight of the credit bureaus measure against the data security regulatory frameworks in other sectors of the economy, such as retail, hospitality, education, and such, what is your view of that?

Ms. SPONEM. I don't know where the standard should fall under, but I do believe that those standards should be fluid. For example, with the standards that we followed 5 years ago, if we were continuing to follow those same standards today we would have been hacked by now.

So those standards need to continue to evolve over time and they need the flexibility to be able to do that as people get more sophisticated in being able to penetrate different systems.

Mr. PITTENGER. Sure.

Ms. SPONEM. So where that falls under and on—what that looks like I don't know. But I think it is really an important piece to make sure that we have in place.

Mr. PITTENGER. Yes, ma'am. Thank you.

Mr. Taylor, do you think it is important to empower law enforcement to share information with the private sector in respect to ongoing cyberthreats and attacks? If you could elude on that some more?

Mr. TAYLOR. Yes, absolutely critical. If law enforcement is aware of threats and if companies had that information they could take steps to protect their systems, absolutely critical.

And I think from an industry perspective even following the Cyber Information Sharing Act, I think there has been a cry from the industry generally for more information, particularly from the Federal Government on threats and vulnerabilities that exist today.

Mr. PITTENGER. Yes, sir. And so you would say that there should be greater information sharing among themselves in the industry in the private sector on ongoing cyberattacks?

Mr. TAYLOR. Yes. And I think it has developed historically in a very sectoral approach. The financial services and retail and technology they all have their information sharing and analysis centers and try and share threats amongst themselves. And it is something that is developing and growing over time.

Mr. PITTENGER. Is there anything we should be doing on the Federal level to encourage information sharing?

Mr. TAYLOR. Can you repeat?

Mr. PITTENGER. Is there anything we should be doing on the Federal level to encourage information sharing?

Mr. TAYLOR. Well, this Congress did pass the Cyber Information Sharing Act, which ostensibly was for that very purpose. And I think that we need a reminder to Federal law enforcement to encourage them to share with the private sector information about threats.

Mr. PITTENGER. Yes, sir. Thank you.

Mr. Rosenzweig, who has the enforcement authority for the various data security regulatory regimes? Is it the FTC, the State attorney general, or banking regulators?

Mr. ROSENZWEIG. It is a patchwork, sir. And it very much is sector-dependent. Right now the FTC has significant authority over consumer-facing institutions. States' attorneys general have authority within their respective jurisdictions under Gramm-Leach-Bliley.

There is regulatory authority from the banking groups, HIPAA as well. One of the things that we see, as Mr. Taylor said, is a sectorally developed set of privacy and security rules that has created some uncertainty as where you fit within the matrix, pretty much.

Mr. PITTENGER. Yes, sir. Thank you. Just very briefly then, I would ask you how can we ensure that Americans' data privacy

and data security interests are best served by the national data security breach notification standards?

Mr. ROSENZWEIG. Well, I would start by saying that I don't think that data breach notification is cybersecurity. It is an ancillary to it because it has the collateral effect of embarrassing people. But it only comes after you have failed.

The right way, the primary way, would be to foster standard setting at the NIST that we have been talking about already today and propagate that throughout industry so that we get a best practices level playing field that is a good standard setting model.

Mr. PITTENGER. Thank you.

My time has expired. I thank you very much.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that, we go to the gentlelady from New York. Mrs. Maloney is recognized for 5 minutes.

Mrs. MALONEY. Thank you, Mr. Chairman. I would like to thank you and the Ranking Member for holding this important hearing. And all of the panelists for your truly riveting testimony that underscored the urgency of acting on the Federal level to protect the information of consumers.

I would like to first ask Professor Rotenberg about the importance of breach notification. I think we all agree that when a company is breached and personal information is stolen, consumers should be notified as quickly as possible.

But before they can be notified about a breach, someone has to discover it. Usually it is the company, but sometimes it is discovered by a third party that the company has hired as a vendor who discovers the breach first.

Now, a number of vendors, independent tech companies that have huge platforms, are opposed to this. And personally I think a third party should notify as quickly as possible.

But my first question is if a third party that a company has hired discovers a data breach at the company, do you think the third party should have an obligation to notify the company of the breach?

Mr. ROTENBERG. Well, thank you, Congresswoman, for the question. And the simple answer is yes. We need more breach notification. We need companies to be made aware of when they have problems securing the data they collect.

And I thought a lot about how best to describe the problem and this question in particular. Imagine, for example, that you made your home available to a friend. And the person goes into your house and the first couple days they are there a pipe bursts and you have water pouring all into your house.

Now, let me ask you the question. Do you think they should contact you right away when the pipe bursts and the water is pouring over your house?

Or should they wait a few days or a couple of weeks or maybe to when you get back home and you are looking around and you are saying, gee, what happened here? Oh, well, the pipe burst. Maybe someone should deal with it.

Data breach is actually very much like a pipe bursting. You have lost control over the information that you have a responsibility to

protect. And if you don't act quickly and if you don't notify somebody who has the ability to fix the problem, it simply gets worse.

And as I tried to explain at the outset, the people who are targeting personal data in the United States today are much more sophisticated than the people 10 years ago or even 5 years ago. These are foreign adversaries. They are trying to uncover national vulnerabilities that they can exploit.

I think we need breach notification that is almost immediate but practicable. Seventy-two hours, which the Europeans chose, I think is probably a good target.

Mrs. MALONEY. I thank you for that excellent reply. And in fact, this article that actually the Chairman loaned to me talks about the European Union in May they are enforcing their 72-hour reporting time, which in a sense will enforce it in America, too, with those companies such as Boeing and GM and Chevron and Microsoft, to mention a few, that are international companies. They are going to obviously have to start responding to what the European standard is.

So Europe's data rules are headed to the United States. It used to be, as the financial capital of the world, the United States would set the standard. Now we are rushing to catch up with what the rest of the world is doing in a very important area.

I must say that after Equifax I would say probably half of the people on this panel were breached. And myself included. And it took them 40 days to disclose that 145 million Americans had lost their security.

And I agree with you that the 30 to 60 days that companies in America are demanding is just too long. I think we should move to the European standard and actually it is being forced on our people now through the law that is going to start being enforced in May from the European Union.

I ask unanimous consent to place in the record this important article that shows the fierce urgency of acting now to move forward on it.

Chairman LUETKEMEYER. Without objection.

Mrs. MALONEY. I will say I talked to the Ranking Member and he is going to join me with some questions that I would like to get everybody in writing because we don't have much time. We have 5 minutes. And I spoke to the Chairman and he said if he approves will join us, which would be great, on getting everybody on record on some of these things.

I can't even be left alone in a hearing. It is going off. Anyway, so I would like to ask Nathan Taylor, you mentioned in your testimony that some States sometimes have data breach notification laws that are inconsistent and directly conflict with each other.

I will give you an example. You noted that some States require companies to tell consumers as much information as possible, while others say you can't. So we need a uniform.

My time is expired. I look forward to sending each of you a thank you note for your excellent testimony and some other additional information that we can see if everybody is onboard on certain changes that we as a Nation should move forward on.

Thank you so very much. I yield back.

Chairman LUETKEMEYER. The gentlelady's time has expired.

With that, we go to the gentleman from Colorado, Mr. Tipton, recognized for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman and thank the panel for taking the time to be able to be here.

Mr. Cooper, I would like to follow up a little on my colleague Mr. Rothfus' question in regards to some consumer confidence. Obviously if we don't have confidence in the data being able to get out into other hands, we undermine the entire process in the eyes of the consumer.

You had cited one instance to be able to help restore some of that consumer confidence by just notifying the people that a breach had occurred. Are there other measures that we should take as well?

Mr. COOPER. Yes. So I think one of the best aspects of both the proposal for legislation in this area and even this hearing is raising the visibility of the importance that anybody who is a steward of data is responsible for making sure that they take reasonable steps in order to keep that data secure.

It is important for what Ms. Sponem's credit union does. It is important for what our members do, because 90 percent or so of data breaches can be prevented just by having good cyber hygiene.

And if more companies are adopting a NIST style framework in order to make sure that they are protecting their data, that they are making sure that passwords are protected, that credentials are protected, will resolve a lot of the data security incidents that we see.

Mr. TIPTON. Thank you. And maybe as a little follow up on that, and Ms. Sponem and Mr. Taylor you might want to weigh in on this as well when we are talking about who is responsible. Can you explain the way in which institutions, which third parties, retailers, who is responsible for the costs of a breach?

Ms. SPONEM. Yes, so today the financial institution is responsible for any entity that is breached that impacts our members negatively. So if it impacts their credit card or that depletes their debit card checking account, we reimburse our members for those fraudulent charges.

In the case of loan fraud, we also do all of the reimbursing of any fraud that takes place from a fraudulent loan. We have increased our costs from trying to identify more fraudulent loans as that has been on a large increase over the last year.

And so things that we might do is make sure that the Social Security number issuance matches date of birth. We will check I.P. addresses on the loan apps to make sure that the I.P. address is from the same State.

We looked up people on social media to make sure that the details match. We check driver's license numbers on the DMV website. So we have gone to great lengths now in 2017 to protect that information, to protect our members from fraudulent loans being made.

And I believe that those entities that are negligent in protecting consumers' data ought to be held responsible for the costs of those data breaches.

Mr. TIPTON. Mr. Taylor?

Mr. TAYLOR. Yes. Statutes today don't define liability. This is a heavily litigated issue, whether it be among companies for a com-

pany's fraud losses or a consumer's losses. That is something that is pursued in courts today to define the liability.

Mr. TIPTON. OK. So ultimately right now liability is landing literally with the banks, with the retailers and we need to have that apply to a little bit more on a broad base? Would that be fair to say?

Mr. TAYLOR. I think liability is an extremely controversial issue. My personal view from my practice is I would tend to lean toward leaving it to the private sector to work it out amongst themselves and define and allocate risk.

Mr. TIPTON. Great. Go ahead.

Ms. SPONEM. I believe that companies who do not take the added steps in protecting consumer data ought to pay for it. I don't know why we would want the banking industry to be at the risk of all of these different entities that are not protecting consumers' data.

And oftentimes ending up in identity theft, which is a much greater problem for consumers.

Mr. TIPTON. Do you have any ideas on really how much we should be spending? A broad-based question, obviously, in terms of cybersecurity. Much of the resources should be allocated for cybersecurity in businesses?

Mr. COOPER. If I may? I would say that it really depends on the type of business that we are talking about. A local restaurant probably has a different amount of resources that it should be putting into its cybersecurity than a web hosting company or a financial institution or a large multinational company that collects and maintains a lot more data.

So I think one of the keys in having a data security set of rules is that they be flexible and scalable depending on the type of company that we are talking about.

Mr. TIPTON. Great. Thank you.

I yield back, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman yields back.

With that, we go to the distinguished gentleman from Georgia. Mr. Scott is recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman. Panel, a very good discussion, really very enlightening, but I tell you, I am very worried. I am worried about the future of our Nation. It seems that we are in a cyber data breach world war. And I think we need to look at it that way.

And United States of America is the number one target.

But I am worried about our inability to adequately respond to this. First of all, you take the fact of Equifax, 145 million people with all of their vital information out in the open, breached upon, and what happens? We first put the consumer protection agency out front doing an intensive investigation and then all of a sudden we draw that investigation back.

There is nothing. I don't know of anybody right now, any Federal agency, that is investigating that breach, especially from a standpoint of even all the information that we had. They waited 2 months before they even notified anybody.

They didn't wait that long when three of their top executives sold their stock once they found out what the breach was and made millions of dollars. No investigation.

You know, I want to ask you, do you think 6 weeks to notify the public of a breach was fair to the American people? Anybody here think that was fair? I don't think so. Everybody is shaking their head that it—do you think that the CFPB should have backed away from this investigation?

Where do you think that the feelings of the American people are resting now? Well, let me ask you this. Under Gramm-Leach-Bliley, do you think that part of the problem may be that there is no delay in notification requirement that is even explicit within Gramm-Leach-Bliley?

Do you think that that may be a part of the problem, Mr. Rosenzweig? Or you, Mr. Cooper? Do we have anything adequate to respond to this?

Mr. ROSENZWEIG. Well, thank you for the question, Mr. Scott. As most of the members of the panel have suggested, the absence of any timeframe requirement for notification it does lead to uncertainty within the marketplace.

I think perhaps unlike some of the other panelists and perhaps some like Mr. Rotenberg in particular, I don't think that a fixed timeframe is necessarily the best answer. I think that sometimes delay is both necessary to ascertain the facts. And sometimes delay is necessary as part of the investigative process underneath the law enforcement interests.

That is not to say that the Equifax delay is an appropriate delay. I don't want to be heard to say that, but for me at least I would prefer a non-determinative, more flexible standard of notification requirement.

Mr. SCOTT. Well, let me ask you, Mr. Cooper, you said in your testimony that data security is a shared responsibility. What did you mean by that?

Mr. COOPER. When a company is collecting and using data, and it might be using another company to help store it or process it, provide customer relations management tools, H.R. tools, there is a need to protect the infrastructure. There is also a need to protect the passwords and credentials that are being used to access that information.

And it is different companies that have different responsibilities as part of that security system. It is—

Mr. SCOTT. Now, let me ask you maybe it seems like right now from my observation we have a hodgepodge of different regulations, different agencies. Wouldn't it be good for us to start trying to figure out how we can zero in and harmonize and get at this in a targeted way to protect the American people's information?

Mr. COOPER. I think having the Federal Trade Commission have the lead responsibility to make sure that reasonable security measures are being taken and that notice is given to consumers when there is a breach in a reasonable amount of time will help make sure that there is timely notification because there is the Federal Trade Commission there to say if you have not provided notice when you should have in a reasonable amount of time, the FTC has enforcement authority.

Mr. SCOTT. Thank you, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that, we go to the gentleman from Texas. Mr. Williams, recognized for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman and also Ranking Member Clay. I want to thank you for holding today's hearing. As we have seen in the past year cybersecurity breaches and the loss of personal identifiable information unfortunately continues to affect hundreds of millions of Americans. The Equifax breach being the largest example.

Now, bad actors are not stopping, in fact, quite the opposite. Organizations around the country continue to be under constant threat from cyber thieves seeking to steal personal data. Our constituents expect us to, where appropriate, consider solutions which successfully defend their information and let them know in the event it has been compromised.

Thank you to the witnesses. It has been good testimony today before us this morning as this committee continues to work to find the answer in the space of consumer information safety and breach notification. And your expert testimony is welcomed.

Ms. Sponem, thank you for being here today to provide the perspective of credit unions in the data security debate. I am a small business owner back in Texas, have been for 46 years and a steadfast defender of Main Street. I am glad to hear from you.

And as you point out in your testimony, data breaches are becoming all too common. We have talked about that. And the cost to institutions like yours have to bear, to fix problems that weren't any fault of your own, begin to add up.

So we have talked a little bit about this, but expand on it. What kind of standards should merchants be held to? And will those standards effectively reduce the cost your institution must pay to assist members who are affected by merchant data breaches?

Ms. SPONEM. I believe that merchants and other businesses that hold consumer information should have the proper controls in place as well. It is the making sure that your patches are done in a timely manner, that you have the proper people in place to monitor those controls and to make sure that you are doing what you need to do to protect that data.

I think that that is at what level of standards? I think that that is something that others will need to decide, but given the type of information that someone holds about consumers I think does, as Mr. Cooper mentioned, does indicate to what level they need to be protecting that data.

Mr. WILLIAMS. OK. Thank you.

Mr. Taylor, in your testimony you recognized the harm that data breaches cause the American consumer. There exists today various State laws regarding the protection of consumer personal information and breach notification in the event that information is compromised.

You are in support of a nationwide breach notification standard, so I ask this. Why is a nationwide Federal breach notification standard the correct policy rather than letting the States govern themselves?

Mr. TAYLOR. Well, I think it ultimately comes down to—and the Chairman in his opening statement said we can't forget about the

consumer. And that is a point that I agree with. This is fundamentally about equal treatment for all Americans, regardless.

A lot of my family lives in Idaho Falls, Idaho. I live in Virginia. Our Social Security numbers are equally sensitive regardless of where we live and the expectation should be the same for companies regardless of where the company operates to protect all of our Socials.

Mr. WILLIAMS. I have another question for you. In your testimony you discuss the steps a company takes in determining the scope of breach. You say that while it would be simple to confirm the facts of what happened, in actuality it takes detailed review before a company can figure out what happened and how to address the breach.

One potential consideration that needs to be made when codifying a breach notification standard is the fact that, as you point out, when the breach becomes public a company becomes a target for other attackers.

So how long would a company be given to secure their systems before being required to make a public notification? And is there a risk that notification could happen too quickly and invite new attacks?

Mr. TAYLOR. There is absolutely a risk. And speaking from my experience alone; one, there is a fundamental point that I would like to highlight, which is all breaches are not created equal. They are really fact-specific.

And so going down the road of picking times, whether it be days or hours, is really challenging because the breaches aren't alike. And it does take time, of course depending on the facts, to both investigate, restore the security of systems and that should be critical.

And our expectation should be that a company should expeditiously investigate and take steps to protect their systems. That is mission critical in my mind.

Mr. WILLIAMS. OK. Thank you very much.

And I yield my time back, Mr. Chairman.

Mr. ROTHFUS [presiding]. The Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

I thank the witnesses for appearing as well, and am concerned about the liability aspect of this that my colleague across the aisle raised earlier.

We seem to believe that there should not be a standard with reference to a timeline for reporting a breach, but we don't seem to think that there should be some sort of liability if that timeline is too long. If you wait until people are suffering such that they could not take some sort of action to help correct.

Now, I think that businesses ought to be able to work out their problems, but what do you do when they don't? What do you do when they have millions of people at risk and their shareholders, some of whom happen to be in some pretty significant positions, my friend Mr. Scott mentioned it, they go ahead and sell their stock before they announce the breach.

Now, if you think that it is appropriate for Equifax to have shareholders in significant positions, let us call them executives, to

allow them to sell their stocks—probably can't stop them—but for them to sell their stocks before the breach is announced, if you think that is appropriate raise your hand, please?

Let the record reflect that no one has indicated that this is appropriate. So when this occurs should there be some sort of liability? Do you think that people ought to be allowed to do this with impunity? Do you think that the poor guy who may not be able to afford a lawyer is going to be able to stop this?

Do you think that class actions are going to be the solution when we have a class of people right here in Congress who are fighting class actions, don't want lawyers to be able to bring class actions against these mal actors?

So what is the solution? To debate it and do nothing? Why wouldn't there be some liability imposed if you knew or should have known that your security measures were inadequate and somebody is suffering as a result?

So let us start with Mr. Rosenzweig.

Mr. ROSENZWEIG. Well, Mr. Green, thank you for the question. I would like to divide the answer. I don't know the facts of the Equifax case. They are still under investigation, but assuming the facts—

Mr. GREEN. Well, let us not talk about the—

Mr. ROSENZWEIG. —that you proposed—

Mr. GREEN. Well, let us do this. Let us take them off the table.

Mr. ROSENZWEIG. Right.

Mr. GREEN. And we will have our own fictitious entity.

Mr. ROSENZWEIG. I would say that insider trading is already a crime. And if you trade on insider information that is an investigation that is appropriate for the SEC and securities enforcement authorities.

I think that that is different from a generalized breach notification law. And there I think that I agree with Mr. Taylor, that the standard is or ought to be a flexible one that reflects expeditiousness at the most earliest reasonably practical time. The law is filled with flexible standards like that, the tort liability standard, for the reasonable man sort of thing.

I do tend to think that firm—

Mr. GREEN. Excuse me. Let me intercede—

Mr. ROSENZWEIG. Sure.

Mr. GREEN. But what should be done when the flexibility that you speak of is abused?

Mr. ROSENZWEIG. Either an administrative enforcement action or possibly litigation. Those are the two possible—

Mr. GREEN. Well, who pays for the litigation?

Mr. ROSENZWEIG. Presumably the people who are litigating.

Mr. GREEN. Would that be the consumer?

Mr. ROSENZWEIG. We don't have a loser pays law here in the United States, so yes.

Mr. GREEN. It would be the consumer. Why wouldn't Congress intercede and establish some standard that deals with this notion of flexibility? Let us assume that you are right. Different circumstances require different timeframes. But what happens when that is abused?

Mr. ROSENZWEIG. Well, that would be a matter for administrative enforcement presumably through the FTC or in the case of Equifax through the banking regulatory authorities.

Mr. GREEN. And I assume that Mr. Taylor you would like to weigh in on this as well?

Mr. TAYLOR. Yes. Throughout this hearing liability has come up in a couple of contexts. And what we have been talking about, two completely separate issues. And the point that you were raising, Congressman, is a good one.

If we are going to have a strong standard, we should hold companies accountable to that standard. And in your bill you can provide penalties that you believe are appropriate for failure to comply with the standard.

There is a separate liability issue that we have talked about in other contexts today, which is the liability between companies who when one company has a breach there can be impacts, for example, to a credit union for reissuing cards. Those are two separate things.

But on the former, I completely agree with you that we should hold companies accountable. If we are going to have a Federal standard we should expect that they comply. And if they don't there should be penalties.

Mr. ROTHFUS. The time of the gentleman has expired.

Mr. GREEN. Thank you.

Thank you, Mr. Chairman.

Mr. ROTHFUS. The Chair now recognizes the gentlelady from Utah, Mrs. Love, for 5 minutes.

Mrs. LOVE. Thank you so much. A few months ago, one of our cybersecurity experts here at the Congressional Research Center, Chris Jaikaran, testified before the Senate Banking Committee about data security. He outlines a process by which organizations typically respond to a breach, and I would like to unpack that a little bit and get your thoughts on various aspects.

Mr. Jaikaran said that there will be a delay between the discovery of an attack and public notification of that attack because the analysis of what has transpired would need to be conducted.

This analysis will inform the entity of how they were breached and what data systems were compromised is what he said. Now, I understand that clearly an organization needs to know what happened before they can accurately notify people who were affected by the breach.

But can we say that this is obviously a theme that I think both sides of the aisle are incredibly concerned about. We hear it over and over and it is asked in so many different ways I can't even imagine your heads must be spinning. But can we say that there should be general parameters on the timing of notification?

Mr. Cooper, I knew you wanted to say something earlier. You pushed your button, so I am going to let you go ahead and answer that question.

Mr. COOPER. Thank you. Yes, so I think that the complexity of the breach is going to affect when notification can happen in an accurate way. And I think accuracy is really important.

I think that it is important that the Federal Trade Commission, and perhaps State attorneys general, are able to enforce a reasonableness standard in terms of the time when notification is pro-

vided so that we can figure out the parameters of what is reasonable and make sure that companies are held to that standard of reasonableness with no enforcement isn't a real standard.

A standard that allows enforcement and penalties when it is not met will help make sure that there are not delays that are unnecessary.

Mrs. LOVE. OK. So there are some serious questions, for example, about the lack of notification regarding the Equifax breach. I would like to get your thoughts, Mr. Taylor, on that because I think one of the analogies that was expressed about pipe breaking in your home, to me the difference is when information is released and what type of information is released.

And I would tend to think that there would be some sort of information saying, you know what? There is a pipe that broke. We don't know how. We will give you further information later about that. But there is a problem and we need to notify of that problem.

So I guess I would like to just get your thoughts about regarding the notification, for example, and the lag of notification, because that is the serious concern here.

Mr. TAYLOR. I appreciate your concern. And while I can't speak to Equifax specifically, I think what the fundamental issue here is, when does the clock start ticking. And I walked through this in detail in my written testimony.

When does a company, quote, "discover a breach." Is that the first awareness of a fact that later with the benefit of hindsight is concluded to have been related to the breach? Or is it the moment that the company determines something is wrong? We have an issue here.

And my point is there should be an expectation that a company expeditiously investigates to figure out what happened and restore the security of their systems and that is, in my mind, when the clock should start ticking, once those steps have been done.

Mrs. LOVE. OK. So when a breach occurs, should there be a specific timeframe for notification established in law? Is there something that we should do to make sure that there is some sort of a timeframe?

Mr. TAYLOR. If by timeframe you mean something like days or hours, I would say no. I think you should go with a standard that is as expeditiously as possible or as as reasonably as possible. I think you need a flexible standard because all breaches are not created equal.

They are very different.

Mrs. LOVE. Is it realistic to require that any company notify customers within a set number of days or whatever circumstance? Is there some sort of reasonable standard that should be out there?

Mr. TAYLOR. I think, again, it really depends. It depends on the facts. A company needs to know whose data was lost in order to be able to notify the right consumer. You don't want to notify the wrong consumer and unduly alarm them. So it—

Mrs. LOVE. So I have just a few seconds, but I just want to say that we are here on behalf—I believe—I keep saying this. The branch of Government that is closest to people is the House of Representatives. And we will not be doing our job if we are not looking

out for the people whose intellectual property has been breached and released.

So our job is to protect the people. It will always be that. And so I think it is our responsibility to make sure that there is something that we can protect people when their information is out—has been breached. So with that, thank you.

Mr. ROTHFUS. The time of the gentlelady is expired.

The Chair now recognizes the gentleman from Washington, Mr. Heck, for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman.

So I want to get at this issue of what do we do about data breaches, and I want to think outside the box a little bit. I am reflecting back on the Equifax breach, and part of which I found incredibly galling, namely that the company essentially threw one person under the bus.

I don't know if that was motivated by a liability limitation, but I thought it was exceedingly poor form. But it was also galling, frankly, because it suggested that something that was so mission critical was dependent on one single individual, which seems to be a systems issue.

But I got to thinking about the gold standard that we have all around us in even more tragic circumstances. Not that this one wasn't tragic—and that would be the National Transportation Safety Board, which is charged to go in after accidents of trains or planes and do the investigation.

Why did this happen and what can we do to prevent it in the future? And there is also a chemical safety board for chemical spills, oil platforms, and the like. That is their sole job. Go in and look at why this thing happened and what can be done to prevent it in the future.

So I got to thinking. A computer network safety board, an entity, a Federal Government entity whose sole job would be to determine how did this come about and what is it that needs to happen in order to prevent it going forward?

So just going down the line there, I am interested in your reaction to that idea.

Mr. ROSENZWEIG. Which end are you starting at?

Mr. HECK. Yours, sir, because you were nodding the whole time I was talking.

Mr. ROSENZWEIG. Well, no. I mean—it is actually an idea that I have been toying with myself. I would say that the only problem that I see with it, serious, is that cybersecurity is really two components. There is the systems approach portion of management of the company protocols in place, awareness of the issue, risk assessments, that sort of thing.

And then there is the technical piece of—did you fail to patch? Was the intrusion detection system inadequate, that sort of thing.

So as you went forward, we would want to do both and the problem, which is very much mirrored in the NTSB, is that the form of those, the human system part is a lot harder to evaluate with precision than the latter.

The NTSB can say part A failed, but they can't say that the company didn't inspect frequently enough because frequently enough is a flexible standard that—

Mr. HECK. But—

Mr. ROSENZWEIG. —but I like the idea generically.

Mr. HECK. But we have human error on the transportation front, too.

Mr. ROSENZWEIG. Right.

Mr. HECK. And I am not understanding why you think the analogy breaks down?

Mr. ROSENZWEIG. I don't think the analogy breaks down. It is just the way you phrased the question at least made me think that you were thinking only of the technical side of the problem.

Mr. HECK. No. No.

Mr. ROSENZWEIG. OK. Then so long as we are willing to accept that human error is human error and can't be—

Mr. HECK. Sure.

Mr. ROSENZWEIG. —eradicated from any human system, I—

Mr. HECK. Right.

Mr. ROSENZWEIG. —I would follow you down this road.

Mr. HECK. Good.

Mr. ROTENBERG. Well, sir, I am going to give you a different answer. I don't think we need another entity responsible for computer security. I think the problem right now is that there is overlapping authority that needs to be clarified.

Both the FTC and the Consumer Finance Protection Bureau have responsibility for security standards. But it is not a mandatory standard and that is part of the problem. I suggest in my testimony that that authority which currently exists should be strengthened.

I also want to mention, and I mentioned this in the testimony, I was very concerned when I read the news reports that the acting director of the CFPB, Mr. Mulvaney, has apparently decided to discontinue the investigation of Equifax when his agency already had the authority to pursue the matter.

Now, why this is of particular concern is not simply about compensating the individuals for whatever harm they have suffered. But it is now almost 6 months since one of the greatest data breaches in U.S. history has occurred and we still don't know who is responsible.

That is actually a remarkable fact. It is as if we went through 9/11 and didn't know who was on those planes. I remember that day. And I almost can't believe that at this moment in time we still don't know who is responsible for the Equifax attack.

So I would say that rather than create a new authority we should make sure that current authorities should do their job. And the last thing that a current authority should do is drop an investigation that it already has the authority to pursue.

Mr. HECK. I am virtually out of time. Sorry to the rest of the panelists. I am sure that you have something meaningful to add as well.

Mr. ROTHFUS. The gentleman's time expired.

The Chair now recognizes the gentleman from Georgia, Mr. Loudermilk, for 5 minutes.

Mr. LOUDERMILK. Thank you, Mr. Chairman and I appreciate the panel being here after spending nearly 30 years in the IT industry and a lot in data security, this is a critical balance that we have

to strive here because as I have heard in here stated several times, it is very difficult.

And Congress cannot respond in the appropriate timeframe for stringent regulatory or stringent regulations for something that moves as fast as technology.

It is impossible for us to keep up with it. And having a hard set Federal standard that meets everything would be like the EPA trying to regulate the security exchanges. It just isn't going to fit in every situation.

So our struggle is how do we ultimately protect the consumer? And as we have seen time and time again, we have to continue to review regulations, especially when you are dealing with financial services.

If you over-regulate what happens is the businesses then are more concerned with meeting the legal standard of the regulation instead of actually doing what is best for the consumer.

But yet you have to have some type of guideline. And that is where I think our struggle is here. Where is that balance? How do we get to that balance?

And it is, as Mr. Taylor said several times, no breaches are the same. They are very unique based on the platform, the diversity of systems, the type of industry, or even the source of the breach.

And that is what we are struggling with a lot now is who is liable? And in the current system it is not always those that caused the data to be breached that are ultimately liable for the consumers and the cost that they are facing.

So I think for me it is looking for what is that stringent guideline or standard that can be flexible. And I think that is what I am hearing from a lot of the panelists here is the flexibility but one that is stringent enough that can go across the multiple platforms.

Because what we are looking at now is totally something different than what our founders ever envisioned. Through federalism you have States had banks. Though history the State of Georgia, when I was in the State legislature, we regulated banks.

Well, they regulate very few banks now because the Federal Government is doing it because they cross so many platforms and money is not transferred by Wells Fargo wagons anymore. It is transferred instantaneously through data networks, which brings in more people who with more liability and more chances for this to be disclosed.

One of the issues that I have spoken about quite often coming from this background is basically a principle we had when I was in the military dealing with intelligence data, was you don't have to secure what you don't have. In other words, don't keep a bunch of stuff.

And one of my concerns that we have is in the Government we require so much data to either be reported to the Government or to be held by companies that really you don't need to keep in an archive that makes us more vulnerable.

Mr. Cooper, with the different standards across the different States, and I understand this, very difficult for businesses, even small businesses. My business we worked in multiple States.

It is very difficult for businesses to know which, really what standard each State has. When it comes to personal identifiable information, do we have multiple definitions of that through States?

Mr. COOPER. Yes. Different States have different definitions of what type of personal information triggers a notification requirement. Perhaps more importantly, there are only a dozen or so States that have data security rules in the first place.

And I think you put your finger on exactly what the difficulty or the art is in what you are trying to do here, which is how to establish a flexible security standard where that flexibility also scales up as time goes on, because as you point out, the types of threats that we are going to face 10 years from now are different than the ones that we face today.

And a flexible standard should make sure that the requirements also ratchet up as we are aware of those threats.

Mr. LOUDERMILK. Well, let me add another aspect into that, because one of the things we don't hear a lot about right now is are we aggressively going after the bad guys? Are we pursuing that aspect?

OK, there is the prevention aspect, but one of the ways of preventing is also prosecuting. Are we putting enough effort into actually going after the criminals who are creating these problems?

Mr. COOPER. So I think it is a really important point to highlight that in these data breaches they are always criminal acts. And making sure that law enforcement does have not just the direction that these are priorities, but also the resources and the institutional knowledge to be able to do the forensics that is required in order to catch them.

It is very difficult, and there are different kinds of breaches and we need to recognize that there are breaches that are from sophisticated actors, some nation-state-linked, some not. There are also much less sophisticated activities that still have a significant impact on all the companies that we are talking about in every industry sector because every industry is relying on data in some way.

Mr. ROTHFUS. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Tennessee, Mr. Kustoff, for 5 minutes.

Mr. KUSTOFF. Thank you, Mr. Chairman. And I do thank the witnesses for appearing today at this very important hearing.

Mr. Rosenzweig, if I can, we have talked about these disturbing cyberattacks that we have seen throughout the last several years. We have talked about Equifax this morning, which affected almost 145 million Americans.

And of course their data has likely been sold on the dark web to somebody.

With Equifax and with other breaches, with Target, with the Office of Personnel Management, information being sold throughout the Internet, it is clear that indeed our financial institutions are clearly vulnerable to attacks.

And as much as we look to do to prevent them, these perpetrators still look for weaknesses and firewalls and other data protection mechanisms.

We have talked today about a national standard or a Federal standard. In your opinion, if Congress years ago had already en-

acted such a standard as you and some of the other witnesses have talked about today, do you think that these breaches still would have occurred?

And if the answer is no, can you talk about how it should be structured or could be structured?

Mr. ROSENZWEIG. I think the answer is yes, the breaches still would have occurred. Maybe not the exact same sets of breaches, but data breach notification law is an after-the-fact amelioration of the harm that has already occurred. The existence of data breach notification laws in 48 States and throughout Europe and throughout the world has not stopped the prevalence of cybersecurity breaches.

What is necessary or what is appropriate to try and implement to limit or reduce the amount of cybersecurity breaches since, of course, they can't be eliminated altogether, is some form of primary standard setting that requires and addresses and advocates for people to raise their game, to bring up the nature of what they are doing so that they are more secure overall.

That includes deploying firewalls and intrusion detection systems. That includes process management systems so that corporations have an awareness of and do risk assessments on their companies.

Those sorts of steps are the primary way of fixing the cybersecurity data breach notification is about privacy and it is about ameliorating the harm after it has occurred. But it is not a primary way of achieving cybersecurity. It is derivative.

Mr. KUSTOFF. Thank you very much.

Ms. Sponem, as we look at banks and credit unions, I am interested in how our financial institutions identify and address cyberattacks when they occur. And as the President of the Summit Credit Union can you discuss the systems that your institution has in place to detect a data breach or other credit unions? What systems they would have in place to detect a credit breach?

Ms. SPONEM. We have at Summit Credit Union and other financial institutions, we have data intrusion tests done on our systems all the time. And so we test our systems. We hire people to try to hack into our systems and so that we can fix any type of vulnerabilities that we might have.

In terms of how do we detect a breach by another entity that might be impacting our members, sometimes that comes from our members themselves, who report a fraudulent charge. And we start to connect the dots and say, this is interesting. It comes from similar places. Sometimes it is identified by places.

Sometimes it is identified that way. Sometimes we get lists from Visa. Sometimes we read about it into the newspaper. Companies do not tend to be forthright and especially merchants with data breaches, and that leads also to this big time delay in us being able to notify people.

Do we really want consumers to have to worry about looking at their information all the time in order to protect themselves from that? Probably not. If we can get a head's up from a company that their systems have been compromised, that is a good indication for consumers to be able to say, oh, OK. Now I am going to look at this a little bit more closely.

We look at that from all different sources and it is not the same. And from a loan fraudulent activity perspective, that we try to protect our members in many different ways by trying to cross-reference different lists and looking up things to make sure that information is consistent so that we are not issuing fraudulent loans.

Mr. KUSTOFF. Thank you. My time has expired. Thank you.

Mr. ROTHFUS. Time of the gentleman is expired.

The Chair now recognizes the gentlelady from New York, Ms. Tenney, for 5 minutes.

Ms. TENNEY. Thank you, Mr. Chairman, and thank you panel for this really important meeting. Obviously this is a huge issue. A really unusual thing happened in my district recently. We had actually a bank robbery where somebody walked into the bank in a traditional way and reminded me of the old movie, Woody Allen movie, Take the Money and Run. He went into the bank with his soap gun.

But this is interesting that now this is occurring in cyber spaces, so just like watching a sports event from the comfort of your living room, you can now rob a bank and heist millions and billions of dollars just by cyber.

And so I think what my biggest concern is, and obviously I wanted to start with Mr. Rosenzweig about, my concern—a number of years ago I attended a seminar before—it was right about the time New York State—and I am a member from New York State, when the Department of Financial Services was being put together.

And the discussion was now our institutions, our banking and financial institutions or credit unions are going to be asked to hand over their private information which they so carefully secure, their information about their customers, obviously their lifeline, to the State of New York. And the concern over the protection and the ability of the taxpayers to protect this data.

And so that is my concern is that I think we know banks and institutions, and we have heard, obviously Ms. Sponem and others talking about how important it is to protect theirs. But how at risk are we when we hand our data over to the State of New York, for example, and how do we prevent against them being hacked?

We know that Congress and our institutions are hacked numerous times on a daily basis. Now the taxpayers, how do we get around the cost in being able to protect that and still have a regulatory regime in place and the balance there? I don't know if you have an opinion on that?

Mr. ROSENZWEIG. That is a great question. Neither the Federal Government nor the State governments are immune from this problem. South Carolina had a very large breach of their driver's license system a few years ago. I am aware of breaches in California and Illinois as well.

I don't know of any in New York particularly, but I imagine they must have happened. And obviously the OPM breach was far more significant for me personally than the Equifax breach because I lost my fingerprints.

There is no way to guarantee the security of State and Federal databases any more than there is a way of guaranteeing the security of bank breaches.

I think that the answer is much the same as with private entities. That State and local institutions and Federal institutions need to be mandated and forced to up their game so that they give at least the best that they can give us.

Ms. TENNEY. Thank you. I do worry because obviously Equifax was a major factor. It hurt our community and these major breaches.

I am just concerned that we go from the private institution, which obviously has as their most important asset is their customer, to have to give that information up to a Government entity just for regulatory purposes. And we know that governments are not always so reliable.

I might ask Ms. Sponem if you could just tell us a little bit about your viewpoint on dealing with a credit union situation? How we protect it? And especially you have identified in your testimony small credit unions and the risk that you have taken and how you feel about turning your data over dealing with your data when it comes to protecting your customers?

Ms. SPONEM. So we are very careful about who we turn our information over to because we also know that, and why the hearing is taking place, is that other entities are not protecting data in the same way that we protect data.

And so we do not like to turn over any information that is personal information about our members unless we absolutely have to do that.

Ms. TENNEY. Thank you. One last thing, and just if we could go to I would say Mr. Rosenzweig or whoever might have an opinion, what can we do to minimize this risk and exposure on the private sector in terms of what could we put in place in terms of a formation of a bill or a regulatory regime that would help us protect the customer but also protect the asset in the event that we do have to turn data over? I don't know if you—

Mr. ROSENZWEIG. I would give you two quick points, minimization of data. A couple of people have said that. You can't be breached for that which you don't collect. And the second, which is a word that we haven't said at all in this hearing is resiliency, which is plan for the failure.

It will happen and what we really don't have is a lot of good recovery systems.

Ms. TENNEY. I appreciate that because I know you pointed out the obvious to me and it is great to have to deal with a data breach later, but it is already the damage has been done and the horse is already out of the barn.

So I do appreciate that. I think preventing it is to me, and again, I thank you for your comments. I love that we—let us not give the information out.

So in that case it is not going to be a secure—and I still have many of my constituents who refuse to even have a bank account. They are still hiding it in the mattress because they are so afraid of data security.

But thank you so much for the panel and for the Chairman. I yield back. Thank you.

Mr. ROTHFUS. The gentlelady yields back.

The Chair now recognizes the gentleman from Kentucky, Mr. Barr, for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman.

Thank you to our witnesses for your testimony today. I will start with Ms. Sponem. Thank—

Ms. SPONEM. Sponem.

Mr. BARR. Sponem. Thank you. I have heard from many of my credit unions that I represent in central Kentucky about the data breach problem. And can you just tell us once again what the average cost is to replace a debit or credit card?

Ms. SPONEM. So anywhere between $3 and $5 per card, but that is actually the least expensive part of a data breach.

Mr. BARR. Because of the fraud monitoring that you have to engage with, addressing your member calls, and actually helping them navigate ramifications of the breach?

Ms. SPONEM. That is correct. So yes, so the actual talking with our members, talking through the breach with them, what they need to do to rectify the situation to make them whole, but also the actual fraudulent charges themselves fall on the financial institution.

Mr. BARR. Right.

Ms. SPONEM. And so as we talk about the standards for other companies, really what is the incentive for companies to not protect their data or to protect their data if we are going to pay for all of—

Mr. BARR. When you take all—

Ms. SPONEM. —their breaches when we take all of it.

Mr. BARR. When you take on all the responsibilities.

Ms. SPONEM. That is correct.

Mr. BARR. And yet financial institutions like credit unions and community banks, you are subject to the Gramm-Leach-Bliley standards, standards that don't apply to other sectors of the economy. Is that correct?

Ms. SPONEM. We are absolutely held to those standards along with reporting of any type of breaches.

Mr. BARR. So your testimony resonates with me because, as I said before, so many credit unions and community banks in the 6th District of Kentucky have told me that of all of the regulatory pressures that they face and the compliance costs that they deal with, this is one of their very top priorities in terms of additional cost and ultimately who bears that cost.

Ms. SPONEM. We bear all of the costs of data breaches, of if there is a fraudulent loan, any type of fraudulent activity, including wire transfers. We hold all of that responsibility.

Mr. BARR. But then beyond that, who ultimately—where is that cost passed along to?

Ms. SPONEM. Well, because we are owned by our members, we, it is really our members' money that we are spending in these fraudulent situations. And that is $1 million in 2017 that could have gone to other things that would have benefited our members.

Mr. BARR. So consumers, the members of the credit union or a customer of a community bank, they are the ones ultimately that pay for this in the form of higher fees or more expensive financial services?

Ms. SPONEM. They absolutely do, yes.

Mr. BARR. Now, let us move on to—that is the problem. Let us move on to the solution a little bit and the proposed Federal legislation to Mr. Taylor and also Mr. Cooper, if you would?

There seems to be some tension in the recommendations a little bit in terms of the desire to create some certainty and some clarity in terms of what standards merchant community or whoever has to comply with. But there is also testimony here today about the need for flexible, scalable standards and technology-neutral standards. We don't want to create a box so that we suppress innovation.

Can you all help us, as we craft this legislation, reconcile that tension? Yes, we want flexibility, yes, we want scalability. We want technology-neutral. I take that recommendation seriously, but how can we at the same time provide for the merchant community that is responsible for adhering to those standards some clarity and legal certainty?

Mr. COOPER. I think we want it to be outcome-focused. I think the goal of a Federal standard on security should be what steps depending on the size of the entity, the type of personal information they have and the amount of personal information they have, what steps will be appropriate?

And if we have the Federal Trade Commission and State attorneys general all enforcing the same law and the same standard we will get that consistency where it still allows for it to be scaled up or down depending on the type of entity or the emergence of new kinds of threats.

Mr. TAYLOR. I would reiterate the point that you made earlier about the Gramm-Leach-Bliley Act and look at that as a model. And it does include notification standards, by the way. I think earlier someone said that it didn't, but it does.

But the GLBA model is, in fact, one that focuses on the process. It is technology-neutral. You need to think about risk. You need to adopt safeguards that address those risks.

Mr. BARR. And final question, Mr. Rosenzweig, should legislation deny a private right of action? Would a private right of action undermine consistent enforcement and what should be the interface between litigation versus a regulatory compliance defense or a standard compliance defense?

Mr. ROSENZWEIG. I am a little agnostic on that. I tend to favor an administrative enforcement mechanism rather than the randomness of class action and litigation.

Mr. BARR. Anybody else on that?

Mr. ROTHFUS. The gentleman's time has expired.

I would like to thank our witnesses for their testimony today. Without objection, all members will have 5 legislative days within which to submit additional written questions for the witnesses to the Chair, which will be forwarded to the witnesses for their response.

I ask our witnesses to please respond as promptly as you are able.

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the Chair for inclusion of the record. The hearing is adjourned.

[Whereupon, at 11:59 a.m., the subcommittee was adjourned.]

A P P E N D I X

February 14, 2018

Hearing on

"Examining the Current Data Security and Breach Notification Regulatory Regime"

House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

February 14, 2018, at 10:00 a.m.
Rayburn House Office Building
Room 2128
Washington, DC

Testimony of Aaron Cooper
Vice President, Global Policy
BSA | The Software Alliance

Testimony of Aaron Cooper

Vice President, Global Policy, BSA | The Software Alliance

Hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime"

February 14, 2018

Washington, DC

Good morning Chairman Luetkemeyer, Ranking Member Clay, and distinguished members of the Subcommittee. My name is Aaron Cooper, and I am Vice President for Global Policy of BSA | The Software Alliance.

BSA is the leading advocate for the global software industry in the United States and around the world.[1] Our members are at the forefront of the development of cutting-edge cloud-enabled data services that have a significant impact on U.S. job creation and the global economy. I commend the Subcommittee for holding a hearing on this important topic, and I thank you for the opportunity to testify on behalf of BSA.

BSA has for more than a decade supported Congressional action to establish a federal standard for data security and data breach notification. The need for a national standard is now more urgent than ever. The steady drumbeat of high profile security incidents that expose consumers to heightened risks of identity theft threatens to undermine public trust in the digital economy.

Federal legislation can play an important role in restoring that trust by setting expectations for good data stewardship, ensuring consumers receive timely and meaningful notification about security risks, and reducing the complexity of compliance in the aftermath of a breach.

The time to act is now. The need is clear, as are the solutions. We urge you to pass a data security and data breach notification bill this Session.

I. Growth of the Digital Economy

Over the last 20 years, consumers, businesses and governments around the world have moved online to conduct business, and access and share information. This shift to a digital world has transformed commerce, helping companies enter new markets and compete on a global scale. It has delivered unprecedented efficiencies and considerable cost savings to every industry sector.

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

The software industry, and BSA members in particular, are at the forefront of the development of cutting-edge technologies and services that are driving the digital economy, such as predictive analytics, cloud computing, AI, and blockchain technologies. These technologies spur job creation and economic growth, provide significant benefits to businesses, and improve the quality of life for many Americans, as well as people around the globe. These benefits will grow substantially in the coming years.

Last September, Software.org: The BSA Foundation released a study with data from the Economist Intelligence Unit (EIU) that showed the software industry alone contributed more than $1.14 trillion to the U.S. GDP in 2016—a $70 billion increase in the past two years.[2] The study also showed that the software industry is a powerful job creator, supporting over 10.5 million jobs, with a significant impact on job and economic growth in each of the 50 states.

Our economy today—and economic growth and job creation in the foreseeable future—are rooted in digital data. The dropping costs of data storage, alongside the acceleration of data driven innovation by BSA member companies and others, have led to profound new uses of data by enterprises across the economy. Every industry today is improved through the use of software.

In every industry, the analysis of data has made businesses more agile, responsive, and competitive, boosting the underlying productivity of many key pillars of our economy. The economic implications of this software and data innovation are enormous. Economists predict that making better use of data could lead to a "data dividend" of $1.6 trillion in the next four years, and that data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030.[3]

II. The Size and Nature of the Challenge

The public's embrace of the digital economy cannot be taken for granted. Ensuring that customers have faith in the security and privacy of their personal data is vital to ensuring their trust in digital services. And, if consumers do not trust technology, they will not use it.

Unfortunately, the spate of recent high-profile security incidents threatens to erode that trust. These concerns are not just theoretical. In fact, a 2017 Pew Research Center study found that nearly two-thirds of Americans (64%) have personally been affected by a major data breach, and nearly half of all Americans (49%) now feel that their personal information has become less secure in recent years.[4]

---

[2] Software.org: The BSA Foundation, *The Growing $1 Trillion Economic Impact of Software* 5 (Sept. 2017), *available at* https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf

[3] *See* BSA | The Software Alliance, *What's the Big Deal with Data?*, 14 (Oct. 2015), available at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf

[4] Kenneth Olmstead and Aaron Smith, *Americans and Cybersecurity,* Pew Research Center (Jan. 26, 2017), available at www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

Over the past several years, there has been an increase in significant security breaches. The numbers are sobering:

- Symantec estimates that more than 7 billion identities have been exposed in data breaches over the last 9 years.[5]
- A 2017 Ponemon-IBM Security study indicates that the average cost for a company that experiences a data breach is now $7.35 million, up 5% from the prior year, and nearly twice as expensive as the global average ($3.62 million).[6]
- The costs associated with notifying consumers in the aftermath of a breach is just the beginning. The average cost to US enterprises that are the victims of cybercrime now exceeds $20 million per year.[7] Experts forecast that the global cost of cybercrime will eclipse $6 trillion per year by 2021, surpassing the global drug trade and equivalent to nearly half of today's US GDP.[8]
- Consumers also bear the considerable costs of cybercrime. In just the last year, more than 978 million individuals were the victims of cybercrime at an average cost of more than $140 per incident.[9]
- In light of these costs, perhaps the most staggering figure is that experts suggest that 93% of all data breaches are preventable through basic cyber hygiene.[10]

III. Anatomy of a Data Breach

Not long ago, the primary threats to security online were vandals and amateur hackers. They chased notoriety and relished the challenge of defeating security systems. Their calling cards were breaches and denial of service attacks to bring down or deface popular websites. While these problems persist, the stakes are now much greater. The threats are now global, the adversaries increasingly sophisticated, and the motivations far more complicated.

According to the most recent data, insider threats, of both the malicious and careless varieties, continue to account for about one-quarter of all breaches.[11] Breaches involving insiders run the gamut – from the innocent loss of a laptop filled with unencrypted customer data to the outright theft and sale of proprietary corporate data to unauthorized third-parties.

---

[5] Symantec, *Internet Security Threat Report* (April 2017) at pg. 45, available at https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_.

[6] Ponemon -IBM Security, *2017 Cost of Data Breach Study*, available at https://www.ibm.com/security/data-breach

[7] Ponemon-Accenture, *2017 Cost of Cyber Crime Study*, https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

[8] Cybersecurity Ventures, 2017 Cybercrime Report, available at https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

[9] Norton by Symantec, *2017 Norton Cyber Security Insights Report Global Results*, https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[10] Online Trust Alliance, Cyber Incident & Breach Trends Report (January 2018), available at https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

[11] 2017 Verizon Data Breach Investigations Report at pg. 3, available at www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Enterprises must also defend against external threats from actors who leverage the interconnectedness and anonymity of the Internet to commit financially motivated crimes and other forms of espionage. Cybercriminals often use socially engineered spear phishing attacks to lure employees into clicking on links or attachments that infect the organization with malware, or they leverage unpatched vulnerabilities as an initial access point into the targeted network. In their most extreme form, often referred to as "advanced persistent threats," these adversaries can burrow into a victim's network for months, or even years, surreptitiously extracting high value data in a manner that is almost impossible to detect. These so-called APTs are conducted by well-resourced teams of specialists that often are linked to nation state actors.

Despite the variety of threat actors, there remains a high degree of overlap in terms of the tactics that give rise to most data breaches. According to the 2017 Verizon Data Breach Report, an astonishing 81% of hacking-related breaches relied upon compromised and/or weak user credentials.[12] Unpatched software is another common vector of attack, with one study concluding that timely patching could prevent nearly 80% of security incidents.[13]

IV. Business Response to the Data Security Challenge

Organizations that hold sensitive data need to incorporate high standards of risk management. This does not always require adopting extraordinary, excessively costly or particularly cumbersome security measures. In fact, reasonable diligence could make a considerable dent into this problem.

For instance, adoption of robust identity management and access control measures could help to address the 81% of hacking-related breaches that rely on compromised user credentials as the vector of attack.[14] Likewise, adoption of transparent and verifiable software asset management (SAM) practices would help enterprises remain aware of product updates and security alerts that require timely patching to lock-down known vulnerabilities.[15] More effective use of encryption could also greatly mitigate the impact of many data breaches when they occur.[16]

For its part, the technology industry has important responsibilities to respond to this, and BSA's members are leading on several important efforts.

---

[12] Id.

[13] Rob Lemos, *Software Patches Could Prevent Most Breaches, Study Finds* (March 2017), available at www.eweek.com/security/software-patches-could-prevent-most-breaches-study-finds.

[14] Mordecai Rosen, *Cybersecurity Executive Order Targets Two Common Attack Vectors* (May 2017), available at https://www.ca.com/en/blog-highlight/cybersecurity-executive-order-targets-two-common-attack-vectors.html.

[15] Ashley Gatehouse, *What is the Role of SAM in Protecting against Network Breahces?* (September 2015) available at https://blog.crayon.com/what-is-the-role-of-sam-in-protecting-against-network-breaches/ ("[S]oftware asset management can be used to validate that software is patched and updated regularly. These patches fix security vulnerabilities that software has. If it is unpatched an organization should consider it unsafe. According to the Verizon Data Breach Investigations Report (DBIR) for 2015, 99.9% of the exploited vulnerabilities were compromised more than a year after the common vulnerabilities and exposures (CVE) was published.")

[16] Rick Robinson, *The Impact of a Data Breach Can Be Minimized Through Encryption* (October 2014), available at https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/

First, BSA recently released a "Cybersecurity Agenda for the Connected Age."[17] This cybersecurity agenda addresses five important pillars:

1. promoting a secure software ecosystem
2. strengthening government's approach to cybersecurity
3. supporting international standards
4. developing a 21st Century cyber workforce, and
5. embracing emerging technologies.

Each of these pillars includes more specific policy recommendations, many of which are key to minimizing the risk of data breaches. They include developing an industry software security benchmark, strengthening identity management, promoting security research and vulnerability management, providing incentives to adopt the NIST Framework, and targeting investments in emerging technologies to enhance security.

Second, BSA members have been leading advocates of "security-by-design" principles and secure development lifecycle approaches to developing software. This is consistent with the Administration's recent draft "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," which highlights that the technology industry should develop and adopt better tools for building security into the design and development of information technology products, systems and services. Broader adoption of these approaches is critical to defending against the vulnerabilities malicious actors exploit in attacks, including those leading to breaches of personal information. Encouraging broader adoption of security-by-design principles and secure development lifecycle approaches, including by emphasizing them with software developers as well as organizations evaluating software suppliers, can pay significant long-term dividends in defending against data breaches. BSA recently suggested that future versions of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, include such guidance for organizations evaluating software suppliers.

Third, the technology industry must prioritize the development and adoption of more sophisticated tools for managing risks to sensitive networks, including technologies for advanced identity management and authentication, continuous monitoring, data loss prevention, analytics-driven security information and event management, and other emerging approaches to security. BSA members are global leaders in this area. Customers in every industry sector rely on BSA members for innovative solutions that provide layered defenses – from protection at the data and document level to the network and perimeter level – that are adapted to the threats they face and the value of the assets they need to protect.

Fourth, the adoption of cloud-based services and technologies offers another important path for organizations to meet the data security challenge. Cloud computing allows organizations of all sizes to leverage the economies of scale that emerge when computing resources are pooled and the overhead costs associated with the management and maintenance of those resource shared between multiple users. These economies of scale often make cloud computing cheaper and more efficient than the traditional on-premises model. Perhaps most importantly, cloud computing can also be a more secure

[17] BSA | The Software Alliance, *A Cybersecurity Agenda for the Connected Age*, available at http://www.bsa.org/~/media/Files/Policy/BSA_2017CybersecurityAgenda.pdf

option for many enterprises. Just as a bank can better protect the individual financial assets of its patrons, cloud service providers can provide a level of protection for their customers' digital assets that exceeds what most individual companies can efficiently provide on their own. Small and medium-sized enterprises (SMEs) are often unable to invest in significant cybersecurity expertise. Cloud services can help SMEs maintain world-class security while remaining nimble.

Common security features of cloud services include:

- ***Physical Security:*** Certified personnel carefully monitor servers 24/7 to prevent physical breaches. Access to servers protected by systems requiring multifactor authentication (e.g., biometric) and monitored using motion sensors and video surveillance.
- ***Data Security:*** Data integrity ensured through use of state of the art encryption protocols for data at-rest and in-transit. Redundant backups of data in geographically dispersed data centers mitigates risk of loss in the event of power outage or natural disaster.
- ***Advanced Threat Detection:*** Access to enhanced security intelligence leveraged to track, prevent and mitigate the risks of cyber threats. Regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- ***Automated Patch Deployment:*** Automated updating of network security protocols to protect systems from newly identified vulnerabilities.
- ***Incident Management and Response:*** Cloud service providers maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- ***Enhanced Administrative Controls:*** Importantly, customers remain firmly in control of their own data and can establish access and use policies tailored to their organization's needs and regulatory profile. Customers retain control over the data location, encryption key management, and data retention/destruction policies. At the same time, cloud service providers also ensure that the storage of customer data complies with applicable international, regional and industry-specific compliance standards.

While cloud services offer significant opportunities for enterprises to improve their cybersecurity posture, it is important to remember that the responsibility for safeguarding customer data does not end when it is placed onto cloud infrastructure. Indeed, there is no "set it and forget it" cloud security model. Regardless of the cloud deployment model, security remains a shared responsibility for both the cloud provider and the tenant.[18]

V. The Role of Federal Legislation

Federal legislation can improve consumer trust in the digital economy by establishing expectations for data stewardship that will reduce the risk of future breaches and ensure that consumers receive timely and meaningful information when their personal information is compromised. A uniform national framework would benefit businesses and consumers alike. It would replace the patchwork of state laws that are now creating confusion and difficulties, allowing businesses to focus their resources on incident response rather than unraveling the current thicket of compliance requirements.

In BSA's view, the value of a federal standard should be measured against three goals:

[18] Microsoft, *Shared Responsibilities for Cloud Computing* (April 2017), available at https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

1. Minimizing the risk of data breaches;
2. Mitigating the impact of breaches when they do occur; and,
3. Reducing the complexity of compliance.

1. Minimizing the Risk of Data Breaches: Reasonable Data Security Safeguards

Federal legislation should promote better risk-management practices by requiring companies that collect or maintain sensitive personal information to implement reasonable data security practices. The practices should be scoped and sized to the complexity, sensitivity, and volume of personal information on a company's systems, and the nature and scope of its business activities.

It is particularly important to avoid imposing technology mandates, which can undermine strong data security by foreclosing innovative and adaptive approaches to combatting evolving threats. Organizations must be able to deploy appropriate and cutting-edge security measures and technologies to protect themselves and their customers' sensitive data effectively against current and future threats. This would not be possible if the law mandated the use of specific products or technologies. Laws and regulations should focus instead on requiring the implementation of reasonable and appropriate security measures. To the extent specific data security practices are required, they should be technologically neutral and outcome-oriented. To provide consumers and enterprises with added certainty, the Committee should consider whether to provide a safe harbor, or presumption of compliance, for organizations that comply with recognized industry standards for data security risk management.

2. Mitigating the Impact of Breaches: Timely and Meaningful Notification

Because there is no such thing as perfect security, the risk of potential data breaches can never be entirely eliminated. Federal legislation should therefore ensure that consumers receive timely and meaningful notification when data breaches do occur. The notification standard should be risk-based, ensuring consumers receive actionable information that enables them to mitigate the potential impact of data breaches that create risks of identity theft or financial fraud. The standard should also promote good data storage practices by clarifying that data rendered indecipherable to unauthorized entities through use of encryption or other obfuscation technologies does not create such risks.

To ensure that the information consumers receive is meaningful, the notification standard should encourage companies that have experienced a breach to focus their immediate resources on performing a thorough risk assessment and restoring the integrity of potentially compromised systems. Affording companies a reasonable time frame for such efforts helps prevent additional collateral damage and ensures that affected consumers receive the information they need protect themselves from identity theft and financial fraud.

Finally, consumers should generally expect to receive notification from the organization with whom they have a direct relationship. Such a principle promotes good data stewardship, ensuring that entities who collect personal information take a life cycle approach to managing the associated privacy and security risks.

3. Reducing the Complexity of Compliance: Preemption and Meaningful Enforcement

In 2003, California became the first state to enact data breach legislation. Variations of data breach legislation have since been enacted by 47 other states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, creating a patchwork of 52 data breach notification standards that is complicated for businesses and confusing for customers. The variations between the state laws are not trivial. In fact, many states include unique requirements on fundamental issues, including what is considered "personal information," the particular circumstances that trigger the notification obligation, the appropriate method for communicating notices to affected individuals, the required content of those notifications, and even who must be notified and on what timeline.

In the aftermath of a potential security breach, the thicket of state laws creates perverse incentives. At a time when organizations should be singularly focused on remediation, the patchwork of state laws forces them to divert resources to evaluating their obligations under 52 different standards. Federal legislation can help clarify and improve the process and allow industry to do what it does best – focus on improving the security of online systems to prevent future attacks and diminish the harm of any actual breach.

The effort to streamline compliance must be coupled with meaningful enforcement mechanisms. A federal standard should ensure that vigorous enforcement can take place to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. The FTC has a strong track record in that respect. We also support the inclusion of state Attorneys General as enforcers when the FTC has not acted. Enforcement by state Attorneys General in federal courts is an important force multiplier that will improve consistency in the application of the federal standard throughout the country.

VI. The Path Forward

The breach of Equifax last year, which exposed personally identifiable information of roughly 145.5 million Americans, served as a wake-up call about the scope and risk of malicious cyber activity. BSA's members are engaged in daily combat to defend consumers, businesses, and government agencies against these malicious actors, from developing innovative new security technologies to maintaining robust real-time monitoring and intervention against threats. As cybersecurity threats grow increasingly dangerous, it is critical that we establish rational, collaborative approaches to protecting the interests of affected stakeholders to include individual consumers. A uniform federal data breach standard will decrease uncertainty and facilitate rapid and robust responses to significant security incidents; federal guidance on data security will drive stronger security measures across the Internet ecosystem. BSA strongly supports these goals, and we look forward to working with the Subcommittee to achieve them.

STATEMENT

of

Paul Rosenzweig
Senior Fellow, R Street Institute
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

before the

Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
United States House of Representatives

February 14, 2018

Choosing the Right Cybersecurity Standards

Introduction

Chairman Luetkemeyer, Ranking Member Clay, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the question of data security for financial institutions. My name is Paul Rosenzweig and I am a Senior Fellow at the R Street Institute.[1] I am also the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice; a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University where I teach a course on Cybersecurity Law and Policy. From 2005 to 2009 I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

[1] The R Street Institute is a public policy, research and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work. Information about our funding is available at: http://www.rstreet.org/about-rstreet/funding-and-expenditures/, and my Truth in Testimony Disclosure accompanies this testimony.

My testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Much of my testimony today is derived from prior academic work I have done in this field.[2]

In my testimony today, I want to make five basic points, which I can summarize as follows:

- There is good evidence that there is a market failure in the provision of cybersecurity;
- There is less evidence on how best to respond to that through regulation, litigation, tax credit or some other federal program;
- Assuming a regulatory response is chosen, the best structure is one with an emphasis on flexibility and scalability (rather than a more mandatory/top-down version);
- Standards of this sort would have the added virtue of stopping the FTC from regulating by consent decree with all the uncertainties attendant thereto; and
- It will have the implicit effect of a creating a safe harbor – which is a good thing and might benefit from being more explicit.

Market Failure

Recent history is replete with examples of data breaches and the harm they cause. Especially relevant to this committee is the Equifax breach that resulted from poor data security practices (the company failed to apply an available patch) and compromised the sensitive, personal data of over 140 million Americans. Some of the data, like Social Security numbers, cannot be changed meaning that individuals may face a long period of frustration and vulnerability to identity theft. This event was largely preventable had Equifax implemented reasonable security measures such as encrypting relevant data.

The federal government itself has not been immune to cyber-attacks. A few years ago a breach at the Office of Personnel Management compromised records of over 20 million people that also contained sensitive information, such as Social Security numbers and fingerprints. Although it was made public in 2015, the attack occurred more than a year earlier and went unnoticed by OPM.

These attacks are emblematic of the fact that U.S. companies and the U.S. government have been and remain vulnerable to attacks, many of which are by actors linked to nation-states that are adversaries of the United States. Nor are they isolated incidents. As the most recent annual Verizon Data Breach Investigations Report notes, 2016 (the last year for which data is available) saw more than 40,000

[2] *See, e.g.,* Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Praeger Press 2012); Paul Rosenzweig "Cybersecurity and Public Goods: The Public/Private 'Partnership,'" *in Emerging Threats* (Hoover Institution Task Force on National Security and Law 2011); S. Baker et al., "Regulators in Cyberia," Regulatory Transparency Project of the Federalist Society, July 2017. https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper.pdf.

incidents and almost 2,000 confirmed breaches.[3] So make no mistake, cyber threats are real, and recent experience has shown that neither the private nor public sectors are fully equipped to cope with them.

The task, then, is to identify an appropriate response. In considering the appropriate scope for government intervention it is useful, initially, to begin with a theoretical model of when governmental activity is warranted. This is not to say, of course, that the theoretical model governs our decision making, but it often serves as a useful guidepost for examining the question.

As a matter of theory and of ideological commitment (born of the independence that are inherent in the foundations of the internet), most private sector leaders will tell you that there is no need for much, if any, government assistance in the cybersecurity market. The only thing they want from the government is more threat and vulnerability information, and then they want it to get out of the way. A closer examination of the theoretical argument suggests, however, that there is some significant room for governmental engagement and, indeed, explains partially, why so many, frequent cybersecurity failures have happened. The theory runs something like this:

A public good is a good that is both non-rivalrous and non-exclusive.[4] In other words, its use by one person does not affect its use by others and its availability to one person means that it is also available to every other person. Public goods have characteristics opposite those of private goods (since, for example, the sale of a shoe to one person both affects its use by others and makes it unavailable to them). The classic example of a public good is national defense. The enjoyment of defense services provided to protect one citizen does not affect the protection enjoyed by another citizen, and defense services provided to one citizen are enjoyed by all other citizens.

Public goods are, typically, beset by two problems – free riders and assurance. Free-riders arise when an individual hopes to reap the benefits of a public good but refuses to contribute to its creation because he thinks others will do so. The assurance problem exists when people refuse to invest in the production of a public good because they believe there will never be enough cooperative investment to produce the good and, thus, that the investment would be futile.

The classic solution to this conundrum is governmental intervention. When a public good is viewed as necessary but cooperation is unavailing, the government coerces its citizens to cooperate through taxation and provision of the public good.

Security in cyberspace, like physical security in the kinetic world, is a market good. People will pay for it and pay quite a bit. But, as in the real world, security in cyberspace is not a singular good – rather it is a bundle of various goods, some of which operate independently and others of which act only in

[3] *See, e.g.,* Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter, July 26, 2017. https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.

[4] *See, e.g.,* David Schmidtz, *The Limits of Government: An Essay on the Public Goods Argument* (Westview Press: 1991).

combination. Broadly speaking these goods are purchased in an effort to protect networks; hardware; data in transit and stored data from theft, destruction, disruption or delay.[5]

Given the breadth of the scope of the concept of cybersecurity goods, it is unsurprising that different aspects of the bundle may be provided by different sources. Just as some security in the physical world can be purchased directly on the private market, so too in cyberspace many security systems (e.g. anti-virus software and intrusion detection systems) are private goods, bought and sold between private sector actors. They are rivalrous (because their use affects other actors) and excludable (since one can limit their use by other actors). Indeed, evidence from the financial sector suggests that cybersecurity is—to a very large degree—a private good. The question is whether or not it is adequately provided by the private sector.[6]

The answer to that question lies in the conception of externalities. Even if cybersecurity is a private good, this does not mean that government has no role in its production. In many instances, the production of a private good will cause an externality – that is, the activity between two economic actors may directly and unintentionally modify a third-party's cost-benefit analysis.[7] Externalities can be either positive (as when a transaction I voluntarily enter into benefits a third party who pays nothing for the benefit) or negative (when the transaction harms an individual).

Many cybersecurity activities have positive externalities. For example, by securing my own server or laptop against intrusion, I benefit others on the network who are derivatively made more secure by my actions. Indeed, almost every security measure performed on any part of cyberspace improves the overall level of cybersecurity by raising the costs of an attack.[8]

But cybersecurity also has two negative externalities. The first is a diversion effect: some methods of protection, such as firewalls, divert attacks from one target to another, which means that one actor's security improvement can decrease security for systems that are not as well-protected.[9]

The second is a pricing problem: private sector actors often do not internalize the costs of security failures in a way that leads them to take adequate protective steps. When software fails to prevent an intrusion or a service provider fails to interdict a malware attack, there is no mechanism through which to hold the software manufacturer or Internet service provider responsible for the costs of those

---

[5] Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Opinions* 7 (Nova Science Publishers: 2009).

[6] Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 J.L. Econ. & Pol'y 497, 498 (2005).

[7] *See* Roy E. Cordato, *Welfare Economics and Externalities in an Open Ended Universe: A Modern Austrian Perspective*, 2 (Kluwer Academic Publishers: 1992) .

[8] *See* Christopher J. Coyne, *Who's to Protect Cyberspace?*, 1 J.L. Econ. & Pol'y 473, 475-76 (2005).

[9] Kobayashi, "Private Versus Social Incentives" *supra*. Less persuasively, Neal Katyal has argued that purchases of private security goods spread fear, thereby potentially increasing the crime rate. See Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime," *The Law and Economics of Cybersecurity*, p. 202.

failures. Consequently, the costs are borne entirely by the end users. In this way, security for the broader Internet is a classic market externality, the true costs of which are not adequately recognized in the prices charged and costs experienced by individual actors.

Subsidy, Regulation, or Litigation?

Addressing the dual nature of these cybersecurity externalities poses a significant policy challenge. Both cases suggest a role for government. But identifying which externality predominates is essential, since the two types point to different policy solutions. We typically subsidize private goods that cause positive externalities because not enough of those goods exist and we wish to encourage investment. By contrast, we often tax or regulate private goods that cause negative externalities to compel the original actor to internalize some of the external costs. Doing that forces the private actor to reduce the level of production to one commensurate with its true costs, or it subject failures to meet standards to a litigation or administrative response.

In either case, two broad caveats to government involvement in the private sector's provision of cybersecurity merit note. First, as with any governmental interference in the marketplace, public choice theorists suggest the exercise of great care regarding the government's ability to systematically make the right choices. This is because rent-seeking behavior by an economic actor seeking a regulatory or legislative preference will adversely affect decision-making.[10] They believe subsidies, taxes and regulations will not foster the "right" result, but rather the result that concerted lobbying efforts favor—a concern that is neither unique to cybersecurity nor unfamiliar to this Committee.

Second, the pace of technological change has increased exponentially—a factor that is perhaps unique to cybersecurity. But the government's hierarchical decision-making structure allows only slow progress in adapting to this phenomenon and operates far too slowly to catch up with the change. We make decisions at the speed of conversation, but change happens at the speed of light.

Thus, though one may acknowledge the theoretical ground for government regulation of cybersecurity based on the externalities that exist, one may doubt the government's capacity to exercise its authority in a timely manner– especially when it acts in a mandatory way. Put bluntly, by the time the government closes its notice and comment period and reaches a decision, the technology at issue will likely be obsolete.

Of course, the contrary argument is also quite well-known and equally persuasive. Whenever we have chosen to address a pricing problem through litigation, there are difficulties that have been extensively documented. Principal among these is the significant degree of transactions costs. Operating a civil justice system is expensive and participating in that system is equally expensive, if not more so. These costs, unrelated to the merits of litigation, have a strong tendency to distort the market in ways that are

[10] See Gordon Tullock, "Public Choice," The New Palgrave Dictionary of Economics Online (2d ed. 2008), http://www.dictionaryofeconomics.com/article?id=pde2008_P000240&q=rational%20choice&topicid=&result_number=1.

often unanticipated – sometimes preventing necessary corrective litigation and at other times incentivizing litigation without social benefit.

The second, equally well known problem is that litigation systems tend to accentuate rather than mitigate problems of free-riders and assurance. The benefits from litigation are often randomly distributed rather than used to ameliorate actual injury. And, of course, the attorneys often garner windfall profits for activities with relatively modest social utility.[11]

As such, even though the case for intervention in the cybersecurity market is relatively robust, it is fair to say that the evidence supporting a particular approach to that intervention is modest and that choices among the options are all likely to have unintended consequences.

The Right Approach

All of which leads to a singular recommendation: **First, do no harm.** Approach the problem with actions that take modest steps in the first instance and be willing to revisit settled approaches as we gain empirical experience with the problem. In the end, if a regulatory approach is chosen at all, it should be a flexible, scalable standard-setting approach with a light administrative enforcement mechanism, rather than a hard, mandatory approach with a heavy civil sanction. Here are some principles that should guide our effort:

First, we should avoid recapitulating a "Maginot Line-type" mentality that posits that adequate protection can prevent cyber intrusions. Our efforts must include a consideration for resiliency.

Second, our approach should learn from what we are already doing. For example, NERC now sets cybersecurity standards for the electric industry, and the CFATS program has cybersecurity performance standards for the chemical industry. The hallmark of those programs is that they avoid a "one-size-fits-all" mandate and instead focus on adopting standards of performance that scale to the size of the enterprise.

Third, we must be careful that our efforts do not have adverse effects on Internet governance and our international posture. Cyberspace is a borderless domain and an American regulatory system will not mix well with that structure. Already, China argues that its regulation of the internal Chinese cyber domain is "just like" our use of NIST to set standards. We may comfortably laugh that off now, but we will have a much harder time making the public case for internet freedom if our own security standards run at all in the direction of, say, identification requirements (that is, affirmative log-on systems of positive identity), as they likely will.

Finally, we must develop a system that creates more certainty than it does uncertainty. That requires two things: guidance and reassurance.

[11] *See generally*, Keith N. Hylton, Litigation Costs and the Economic Theory of Tort Law, 46 U. Miami L. Rev. 111 (1991).

As to guidance, we need a model that relies on a flexible standard, but also one that is clearly articulated. By contrast, for example, today much of the guidance from the FTC to consumer enterprises on acceptable cybersecurity practices comes in the form of consent decrees that, taken together, articulate an indefinite standard of reasonable behavior. That is a remarkably poor way to set standards.[12]

In the cyber and privacy sector, the FTC has brought over 200 regulatory enforcement actions. Because of the reputational harm, distraction and cost of litigating these matters, many companies will settle with the FTC and sign a consent decree. Such agreements are not subject to oversight or review by courts. In some consent decrees, the FTC takes the view that it should monitor the company for 20 years. In the life of the information economy, 20 years covers the birth, use and death of multiple generations of a technology.[13]

Additionally, if a company wants to stay out of the FTC quagmire, it will struggle to do so because the FTC has issued very little guidance to articulate what "unfair business practices" means. Indeed, the FTC declines to adopt official guidance that would alert businesses to the sort of conduct that the agency considers unfair. As Judge William Duffey, a judge involved in one of the only two cases that have gone to court challenging the FTC's consent decrees, observed: "how does any company in the United States operate when [it asks the FTC] 'tell me exactly what we are supposed to do,' and you say, 'well, all we can say is you are not supposed to do what you did.' ... [Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that."[14] Indeed, it is far better to establish a set of rules that defines a standard in statute and allows for enforcement through administrative measures that are subject to judicial and congressional review.

This leads to the second necessary component of any standard-setting exercise: the quality of reassurance. Put simply, no enterprise will invest resources in achieving performance standards without some assurance that doing so is of benefit to the enterprise. Part of the benefit, of course, will accrue from the enhanced safety that (presumably) follows from the adoption of an appropriate standard of care.

But in reality, a major portion of the benefit will lie in the fiscal security of knowing that the enterprise has taken adequate steps to avoid liability for inadequacy. Perhaps that sort of safe harbor will be

---

[12] For clarity sake I should note explicitly that the FTC example cited here is simply to illustrate an approach I find unhelpful. I am, of course, aware that many of the institutions the committee oversees (banks, credit unions, insurance companies) are expressly exempt from the Federal Trade Commission Act and that the FTC is prohibited under the McCarran-Ferguson Act from playing any role in the business of insurance.

[13] As expressed by Judge Douglas Ginsburg, "The 20-year term seems to be almost certainly inappropriate in high-tech industries with very fast turnover in product design. [...] How many iPhones will there be in 20 years? Twenty years of supervision over that kind of evolution strikes me as completely unfounded." Quoted in S. Baker, et al., "Regulators in Cyberia," Regulatory Transparency Project of the Federalist Society, July 24, 2017. https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper.pdf.

[14] *Id.* The quotation is from a hearing in the FTC's enforcement action against LabMD.

implicit in any standard-setting effort, but it is worth asking the question whether or not an explicit safe harbor might not generate greater uptake. I tend to think it will and that any regulatory or standards-based intervention by the government should be accompanied by a form of verified compliance that is a bulwark against liability and governmental action.

What then should a standard-setting system look like? In many ways, we already have several good models that have been deployed in various federal agencies. The standard setting at NIST, for example, has been a hallmark of a successful effort, characterized by transparency and inclusiveness. The result has been a series of baseline recommendations that are flexible in implementation and scalable in scope depending on the nature of the enterprise. Appropriate standards must not be developed from a hierarchical, top-down perspective, but rather should be the result of a bottom-up approach that recognizes the significant, and often superior, expertise in the private sector.[15]

One final point bears brief mention. As I understand it, the Committee is also considering federalizing data breach notification law. While I am agnostic on the general proposition, one point bears emphasis – data breach notification is not cybersecurity. It is, at best, a second order effort at transparency as a means to foster security, but it does not directly create a safer cyber environment. To that end, I would urge the Committee to insure that its consideration of data breach rules moves in tandem with more substantive and direct consideration of security standards.

Conclusion

We face a wicked problem. Without a doubt, private sector actions will create externalities that the market cannot account for and that cannot be effectively managed by a self-organizing private sector. But the prospect of government action to correct for those externalities raises the same traditional problems of regulatory capture that attend any government endeavor. More fundamentally, precisely because cyberspace is unique in its rapidly changing and path-breaking nature, we face the almost intractable problem of creating policy too slowly to be of any utility. We should neither want to overly diminish the problems nor be sanguine about the capacity to find useful answers. We should, however, approach the problem with a very healthy dose of humility. A flexible, modest, scalable approach is far better than a harsh regulatory mandate and deserves our serious consideration. Ultimately, then, the principal recommendation for government is to treat cyberspace like any patient with an ailment and "first, do no harm."

[15] A less helpful, more mandatory model that should be disfavored was the way in which New York State developed a regulatory framework for financial service companies. *See* Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500. http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime"

Before the

House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

February 14, 2018
2128 Rayburn House Office Building
Washington, DC, 20002

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the current data security and breach notification regulatory regime. My name is Marc Rotenberg. I am President of the Electronic Privacy Information Center ("EPIC"). EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] I have also taught information privacy law at Georgetown University Law Center since 1990 and I am the author of several leading books on privacy law.[2] I testified before this Committee in 2011 following the spate of data breaches in the financial services sector.[3] And in a recent article for the *Harvard Business Review*, I outlined several steps that Congress could take in response to the Equifax data breach.[4]

Data breaches pose enormous challenges to the security of American families, as well as our country's national security. Privacy, more precisely described as "data protection," is no longer simply about companies that misuse or fail to protect personal data. Today our country is facing cyber attacks from foreign adversaries and it is the personal data stored by companies that is the target. When these companies engage in lax security practices or freely disclose consumer data without consent, they are placing not only consumers, but also our nation at risk.

The United States also faces growing challenges on the trade front. Many countries are increasingly concerned about the absence of adequate privacy protection for the personal data of their consumers that is collected by Internet firms in the United States. There is a real risk that over the next year, privacy officials in Europe will move to limit the flow of personal information to the United States unless appropriate legal safeguards are established.

In my testimony today I will outline a comprehensive approach to data protection for the United States. EPIC recommends both comprehensive legislation and the establishment of a federal data protection agency. Congress should enact legislation that (1) gives consumers greater control of their personal data held by others; (2) limits the use of the Social Security Number in the private sector; (3) mandates data breach notification; (4) changes the defaults in the credit reporting industry with (a) default credit "freezes" that give consumers opt-in control over the release of their credit report, (b) free, routine monitoring services, and (c) free access at any time for any purpose to a consumer who wants to see the complete contents of a credit report or other similar information product made available for sale. In addition, Congress should establish a data protection agency in the United States.

---

[1] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html. EPICs Advisory Board includes distinguished experts in law, technology, and public policy, https://epic.org/epic/advisory_board.html.

[2] ANITA ALLEN AND MARC ROTENBERG, PRIVACY LAW AN SOCIETY (West 2016); MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (EPIC 2016); MARC ROTENBERG, ET AL, PRIVACY AND THE MODERN AGE: THE SEARCH FOR SOLUTIONS (The New Press 2015).

[3] *Cybersecurity and Data Protection in the Financial Services Sector: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 112th Cong. (2011) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.

[4] Marc Rotenberg, *Equifax, the Credit Reporting Industry, and What Congress Should Do Next*, Harv. Bus. Rev. (Sept. 20, 2017), https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next. See also, Christine Bannan, *Equifax's Data Breach Sins Live on to This Year's Tax Season*, The Hill (Feb. 1, 2018), http://thehill.com/opinion/finance/371815-equifaxs-data-breach-sins-live-on-to-this-years-tax-season.

There are several proposals in the House and Senate to strengthen privacy protection for Americans. Given the rapidly increasing risks to consumers from data breaches and identity theft, now is the time for Congress to implement much-needed reforms.

I. The scope of the data breach problem

A. Data breaches are an epidemic in the United States

2017 marked yet another "worst year ever" for data breaches.[5] One report found that the number of data breaches nearly doubled from 2016 to 2017, and 73% of all U.S. companies have now been breached.[6] There were a total of 159,700 cybersecurity incidents in 2017.[7] These figures represent a disturbing lack of data security by U.S. companies.

The data breach epidemic imposes an enormous cost on the U.S. economy. According to the Department of Justice, 17.6 million individuals – 7% of all Americans – experienced identity theft, at a cost of $15.4 billion to the U.S. economy.[8] The Department of Justice found that 86% of identity theft victims experienced the fraudulent use of existing account information.[9] A recent report found that identity fraud increased by 16 percent in 2016, with a total of $16 billion stolen from 15.4 million U.S. consumers.[10] Identity theft continues to be the number one complaint to the FTC.[11]

Identity theft can completely derail a person's financial future. Criminals who have gained access to others' personally identifiable information can open bank accounts and credit cards, take out loans, and conduct other financial activities using someone else's identity. Identity theft has severe consequences for consumers, including:[12]

- Being denied of credit cards and loans
- Being unable to rent an apartment or find housing
- Paying increased interest rates on existing credit cards

---

[5] Online Trust Alliance, *Cyber Incident and Breach Trend Report*, (Jan. 25, 2018), https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.
[6] *Id*; *See also*, Thales, 2018 DATA THREAT REPORT, https://dtr.thalesesecurity.com/.
[7] Online Trust Alliance, *supra*, at 5.
[8] Bureau of Justice Statistics, *17.6 Million U.S. Residents Experienced Identity Theft in 2014*, Press Release, (Sep. 27, 2015), https://www.bjs.gov/content/pub/press/vit14pr.cfm.
[9] *Id.*
[10] Javelin Strategy & Research, *Identity Fraud Hits Record High With 15.4 Million U.S. Victims in 2016, Up 16 Percent According to new Javelin Strategy & Research Study*, Press Release, (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.
[11] Fed. Trade Comm'n, *FTC Releases Annual Summary of Consumer Complaints* (March 3, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.
[12] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, http://www.idtheftcenter.org/images/page-docs/Aftermath2017Finalv1.pdf.

- Having greater difficulty getting a job
- Suffering severe distress and anxiety

B. Recent data breaches demonstrate the need for reform

Two recent high-profile data breaches at Equifax and Uber underscore the urgent need for reform. The Equifax data breach was one of the worst in U.S. history. Over 145 million Americans had sensitive personal information stolen, including Social Security numbers, driver's license numbers, dates of birth, and addresses—data that is a gold mine for identity thieves.[13] Equifax was aware of a major security vulnerability in its system but failed to fix the problem for four months.[14] Equifax's data security was so inadequate that a single point of failure exposed the personal data of more than half of American consumers.

Equifax's response to the breach created even further harm for consumers. Equifax waited six weeks to notify the public of the breach.[15] The company then created a website where consumers could find out if their information had been hacked, but the website didn't work, and at one point the company even directed consumers to a phishing website designed to look like Equifax's page.[16] And while Equifax offered free credit monitoring services in the wake of the breach, it initially used this offer to force consumers to sign away their rights to sue Equifax in court, relenting only after public outrage.[17]

EPIC testified before the Senate following the Equifax breach, urging reform of the credit reporting industry.[18] We emphasized in our testimony that as a result of the breach, the incidents of identity theft and financial fraud are likely to increase. The IRS did report that tax-related identity theft fell by 40 percent in 2017—from 401,000 reports to 242,000—in spite of the fact that the rates of identity theft continue to climb overall.[19] However, the Equifax breach creates a risk that the incidents of tax fraud could also climb back up.[20]

---

[13] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), https://investor.equifax.com/tools/viewpdf.aspx.
[14] The Apache Software Foundation Blog, *MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® Struts™ Exploit* (Sept. 14, 2017), https://blogs.apache.org/foundation/entry/media-alert-the-apache-software.
[15] Chris Isidore, *Equifax's Delayed Hack Disclosure Did it Break the Law?*, CNNtech, (Sep. 8, 2017), http://money.cnn.com/2017/09/08/technology/equifax-hack-disclosure/index.html.
[16] Merrit Kennedy, *After Massive Data Breach, Equifax Directed Customers To Fake Site*, NPR, (Sep. 21, 2017), https://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site.
[17] Diane Hembree, *Consumer Backlash Suprs Equifax to Drop 'Ripoff Clause' in Offer to Security Hack Victims*, Forbes, (Sep. 9, 2017), https://www.forbes.com/sites/dianahembree/2017/09/09/consumer-anger-over-equifaxs-ripoff-clause-in-offer-to-security-hack-victims-spurs-policy-change/.
[18] *Consumer Data Security and the Credit Bureaus: Hearing Before the S. Comm. on Baking, Housing, and Urban Affairs*, 115th Cong. (2017), (statement of Marc Rotenberg, Exec. Dir., Electronic Privacy Information Center), https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10-17.pdf.
[19] Aaron Lorenzo, *IRS Reports Drop in Tax-related ID Theft for Second Straight Year*, PoliticoPro, (Feb. 8, 2018), https://www.politicopro.com/tax/whiteboard/2018/02/irs-reports-drop-in-tax-related-id-theft-for-second-straight-year-580230.
[20] Bannan, *supra*, at 4.

In a recent letter to the Senate, EPIC highlighted the fact that CFPB Acting Director Mick Mulvaney has apparently ended the investigation into Equifax.[21] According to reports, Mulvaney has ended plans to test Equifax's security systems, rejected offers from regulators to assist with the investigation, and declined to seek subpoenas or sworn testimony from Equifax executives.[22] This failure to pursue a thorough investigation of the Equifax matter verges on malfeasance.

A data breach at Uber was also the subject of a recent Senate hearing on "bug bounty" programs.[23] Uber's massive data breach in 2016 exposed the personal information of 57 million Uber customers and drivers, including their names, email addresses, phone numbers, and driver's license numbers.[24] Rather than disclose the data breach to the public, as required by law, Uber paid the hackers $100,000 to delete the information.[25] Uber did not disclose the data breach until a year later.[26] EPIC submitted a statement to the Senate in advance of the hearing, and warned that while bug bounties are sometimes legitimate, they do not excuse a company's legal obligation to notify the public of a data breach.[27] The risk that hackers will still user data and hold it for ransom will likely increase.[28]

C. Consumers lack control over their data

The Uber and Equifax breaches demonstrate why the current system is broken: consumers lack control over their own data. As the data broker industry proliferates, companies have enormous financial incentivizes to collect consumers' sensitive personal data.[29] Yet data brokers have little financial incentive to protect consumer data. There are between 2,500 and

---

[21] EPIC, *Letter to S. Comm. on Banking, Housing and Urban Affairs*, (Feb. 6, 2018), https://epic.org/EPIC-SBC-CFPBinvestigation-Feb2018.pdf.
[22] Patrick Rucker, *Exclusive: U.S. consumer protection official puts Equifax probe on ice – sources*, Reuters, (Feb. 5, 2018), https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ.
[23] *Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers*, 115th Cong. (Feb. 6, 2018), S. Comm. on Commerce, Science, & Transportation, https://www.commerce.senate.gov/public/index.cfm/2018/2/data-security-and-bug-bounty-programs-lessons-learned-from-the-uber-breach-and-security-researchers.
[24] Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg, (Nov. 21, 2017), https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.
[25] *Data security and Bug Bounty Programs, supra* at 24..
[26] *Id.*
[27] Letter from EPIC to S. Comm. on Commerce, Science & Transportation, *Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers*, (Feb. 5, 2018), https://epic.org/EPIC-SCOM-UberBreach-Feb2018.pdf.
[28] There are other recent examples of hackers holding personal data for ransom. *See, e.g.* Phil Muncaster, *Over 19 Million California Voter Records Held for Ransom Again*, Info Security, (Feb. 9, 2018), https://www.infosecurity-magazine.com/news/over-19m-californian-voter-records/; Samm Quinn, *Hospital pays $55,000 ransom; no patient data stolen*, Greenfield Reporter (Jan. 15, 2018), http://www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/.
[29] Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability*, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

4,000 data brokers in the United States that collect and sell personal information without consumers' knowledge or consent.[30] For these companies, consumers are the product, not the customer.[31] Companies also maintain information about consumers that is often inaccurate, causing consumers to be wrongfully denied credit, housing, or even a job.[32] Furthermore, consumers face a "black box" of complex, secret algorithms that determine their creditworthiness.[33]

Under the current system, consumers bear the costs when companies fail to protect their personal information. Consumers must contact all three credit bureaus and pay a fee to each company each time they wish to freeze and unfreeze their credit.[34] Credit bureaus like Equifax do not make it easy for consumers to freeze their credit because they profit from selling access to consumer data. And consumers only learn of the breach once the company decides to notify the public.

II. Current law is inadequate to protect consumers

Consumers in the United States face a data protection crisis, and the current patchwork of state and federal laws are woefully inadequate to address the problem. Currently, no federal law requires credit reporting agencies to offer credit freezes. States have enacted their own credit freeze laws, but these laws permit companies to charge fees to consumers to freeze their credit. Fees are typically $10 per credit reporting agency but less in some states. Some states also mandate free credit freezes for protected categories of consumers, such as: spouses of identity theft victims, minors, consumers over 65 years of age, active duty military members, and victims of domestic violence.[35] Some states (Maine, South Carolina, Indiana, and North Carolina) have prohibited fees to both place and remove freezes for all of their citizens.[36] State laws also specify the length of the freeze: it can either be permanent (until lifted by the consumer) or it can expire after a certain period of time. In three states, a freeze will automatically expire after seven years.[37]

At the federal level, consumers have little protection over their credit reports. The Fair Credit Reporting Act (FCRA) entitles consumers to only one free credit report per year, and the

---

[30] *Id.*
[31] Bruce Schneier, *Don't Waste Your Breath Complaining to Equifax About Data Breach*, CNN, Sep. 11, 2017, http://www.cnn.com/2017/09/11/opinions/dont-complain-to-equifax-demand-government-act-opinion-schneier/index.html.
[32] Fed. Trade Comm'n., *Free Credit Reports*, March 2013, https://www.consumer.ftc.gov/articles/0155-free-credit-reports.
[33] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[34] Lisa Weintraub Schifferle, *Free credit freezes from Equifax*, Fed. Trade Comm'n., (Sep. 19, 2017), https://www.consumer.ftc.gov/blog/2017/09/free-credit-freezes-equifax.
[35] ConsumersUnion, *Consumers Union's Guide to Security Freeze Protection,* http://consumersunion.org/research/consumers-unions-guide-to-security-freeze-protection-2/.
[36] *Id.*
[37] *Id.*

process of obtaining one is cumbersome.[38] Additionally credit reporting agencies are only required to "maintain reasonable procedures designed" to prevent unauthorized release of consumer information under FCRA.[39] In practice, this means that credit reporting agencies must take some precaution to ensure that credit information will only be used for lawful purposes, but the Federal Trade Commission has specified that this standard can be met with a blanket certification from the purchaser of the credit report that the report will be used legally.[40]

The Federal Trade Commission has limited data protection authority under the "Safeguards Rule" of the Gramm-Leach-Bliley Act.[41] This rule only applies to financial institutions, however, and the Commission has also failed to make compliance with the rule mandatory.[42] Moreover, Gramm-Leach-Bliley disperses oversight of financial institutions across seven agencies and fails to cover credit reporting agencies.[43] Given that credit reporting agencies hold more sensitive personal data than many of the other financial institutions combined, it makes little sense for those companies to be exempt from the rules.

The Dodd-Frank Act transferred authority over certain privacy provisions of Gramm-Leach-Bliley to the Consumer Financial Protection Bureau, but Dodd-Frank did not give the CFPB authority to establish data security standards.[44] The CFPB, like the FTC, can only bring enforcement actions based on a company's affirmative misrepresentations about data security practices.[45]

III. Congress should enact comprehensive data protection legislation

There is widespread support for data protection legislation among Americans. According to the Pew Research Center, 91% of consumers say that they have lost control over how personal information is collected and used by companies.[46] The same study reported that 64% of Americans supported greater regulation over how advertisers handle their personal data. Even leading CEOs now support stronger privacy protections in the United States. Last fall, I had the

---

[38] 15 U.S.C. § 1681, *et seq*.
[39] EPIC, *Identity Theft*, https://www.epic.org/privacy/idtheft/.
[40] *Id.*
[41] *Standards for Safeguarding Customer Information*, 81 Fed. Reg. 61,632.
[42] *See*, Comments of EPIC to the Fed. Trade Comm'n, *Standards for Safeguarding Customer Information Request for Public Comment*, FTC Dkt. No. 2016-21231 (Nov. 7, 2016), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Rule-Comments-11-07-2016.pdf.
[43] 15 U.S.C. § 6801; *see* 79 Fed. Reg. 37166 (2014) ("Section 501(b) of the Gramm-Leach-Bliley Act (GLB Act) requires the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision (the Agencies), as well as the National Credit Union, the Securities and Exchange Commission, and the Federal Trade Commission, to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to the administrative, technical, and physical safeguards for customer records and information.").
[44] *Id.*
[45] *See, e.g.*, Consumer Financial Protection Bureau, *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices* (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.
[46] George Gao, Mary Madden, Privacy and Cybersecurity: Key Findings From Pew Research, Pew Research Center, (Jan. 16, 2015), http://www.pewresearch.org/fact-tank/2015/01/16/privacy/.

opportunity to speak with leading CEOs from across the country about the Equifax breach. After a brief exchange, the event moderator polled the CEOs and 95% "want stronger consumer privacy laws."

The basis of modern privacy law is "Fair Information Practices" – the rights and responsibilities associated with the collection and use of personal data.[47] These rights and responsibilities are necessarily asymmetric: the individuals that give up their personal data to others get the rights; the companies that collect the information take on the responsibilities. This is the approach that the United States, the European Union, and others have always taken to establish and update privacy laws concerning the collection and use of personal data.

In the section that follows I will outlines the most pressing Fair Information Practices that Congress that should enact.

A. Establish baseline standards for data security

Legislation should require companies to implement certain baseline data security processes, rather than give companies wide latitude to determine what constitutes reasonable security measures. For example, the Florida Information Protection Act requires that companies collecting consumer data "take reasonable measures to protect and secure data in electronic form containing personal information."[48] Companies that collect and store sensitive consumer data are in the best position to prevent data breaches, and they should be held liable when they fail to adopt reasonable security measures.[49] This is especially important because the Equifax hack and other major data breaches caused by known vulnerabilities are entirely preventable.[50]

EPIC supports a data minimization requirement. It has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset.[51] It is the credit card numbers, the bank account numbers, the government identification numbers, and the passwords that draw the attention of computer criminals. Reducing the target size reduces the vulnerability.

B. Require prompt breach notification

---

[47] EPIC, *Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html; ALLEN & ROTENBERG, PRIVACY LAW AND SOCIETY 755-58, 760-64(WEST 2016)

[48] Fla. Stat. § 501.171(2) (2017). See EPIC, State Data Breach Notification Policy (2017).

[49] Brief of Amicus Curiae EPIC in Support of Appellants, Storm v. Paytime, No. 15-3690, at 25–30 (3d Cir. filed Apr. 18, 2016), https://epic.org/amicus/data-breach/storm/EPIC-Amicus-Storm-Paytime.pdf.

[50] See Lily Hay Newman, Equifax Officially Has No Excuse, Wired (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[51] Data minimization obligations, and even data deletion provisions, can be found in many U.S. privacy laws. *See, e.g.,* Privacy Protection Act of 1987, 18 U.S.C. 2710(e):

> (e)Destruction of Old Records.—
> A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

Congress should mandate that companies notify consumers and law enforcement within 48 hours of a data breach. The only federal law with a breach notification rule is the Health Insurance Portability and Accountability Act, which only applies to protected health information.[52] Presently, companies often wait days, weeks, or even a year to notify consumers of a breach. When consumers are left in the dark, they cannot take measures to protect themselves, such as obtaining a credit freeze or monitoring their accounts. There is currently a patchwork of state laws mandating breach notification but no federal standard.[53] Florida has one of the most comprehensive data breach laws, providing a mandatory 30-day notification rule, a broad scope, and proactive requirements for reasonable data protection measures.[54] A federal standard should go even further, but it should not preempt state law, giving states the flexibility to provide additional safeguards to consumers. A breach notification law should also require companies to notify consumers via automated texts, e-mail messages, and social media, as companies are increasingly communicating with consumers electronically.

C. Limit the use of the SSN in the private sector

Social security numbers have been asked to do too much. SSNs were never meant to be used as an all-purpose identifier.[55] The unregulated use of the social security number in the private sector has contributed to record levels of identity theft and financial fraud.[56] The Equifax breach illustrates this problem, as the social security numbers of nearly half of all Americans were stolen. Those whose SSNs have been breached suffer a rate of new account fraud more than six times higher than all consumers.[57] The more the SSN is used, the more insecure it becomes. Out of 1,091 total breaches in 2016, 568 exposed SSNs (52.1% of all breaches that year).[58]

The solution is not, however, to replace the social security number with a national biometric identifier that raises serious privacy and security risks.[59] Instead, we suggest that the best way to minimize the problem of identity theft is to reduce the industry's reliance on the

---

[52] 45 C.F.R. §§ 164.400–414. The Graham-Leach-Bliley Act "Interagency Guidelines" also discuss consumer notice, but the rules do not contain a requirement that notice be given within a specific time period. *See* 12 C.F.R. pt. 224, app. F (Supp. A 2014); 70 Fed. Reg. 15,736 (2005).

[53] *See* National Conference of State Legislatures, *Security Breach Notification Laws*, (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[54] EPIC, *State Data Breach Notification Policy* (2017), https://epic.org/state-policy/data-breach/.

[55] Marc Rotenberg, *The Use of the Social Security Number as a National Identifier*, 22 Comp. & Soc'y nos. 2, 3, 4 (Oct.1991).

[56] Marc Rotenberg, Equifax, *The Credit Reporting Industry, And What Congress Should Do Next*, Harv. Bus. Rev., (Sep. 20, 2017), https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.

[57] Identity Theft Resource Center, *New Account Fraud—A Growing Trend in Identity Theft* at 3 (November 2016), https://www.idtheftcenter.org/images/page-docs/NewAccountFraud.pdf.

[58] Identity Theft Resource Center, ITRC Breach Statistics 2005-2016, https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf.

[59] EPIC, *Identity Theft*, http://epic.org/privacy/idtheft/.

social security number as a personal identifier.[60] Although the SSA and IRS are the only entities with clear statutory authority to use the number, use of the SSN in the private sector has become widespread. Congress should prohibit the use of the social security number in the private sector without explicit legal authorization.

D. Provide consumers with free credit freezes and thaws (change the defaults for report disclosures to "opt-in")

Credit reporting agencies should change the default on access to credit reports by third parties. Instead of the current setting, which allows virtually anyone to pull someone's credit report, credit reporting agencies should establish a credit freeze for all disclosures, with free and easy access for consumers who wish to disclose their report for a specific purpose. A credit freeze is one of the only mechanisms available to prevent "new account identity theft" before it happens.[61] But only four states (Indiana, Maine, North Carolina, and South Carolina) mandate free consumer access to credit freezes and thaws, while four additional states "provide free freezes but charge for thaws."[62] This means that "[a]pproximately 158 million consumers between 18-65 in 42 states and DC must pay a fee to get credit freezes."[63]

E. Give consumers a private right of action and eliminate mandatory arbitration

The most effective way to improve data security is to establish a private right of action for consumers who have suffered a breach of their personal data. This provides a specific remedy for a specific harm. U.S. privacy laws routinely provide statutory damages.[64] Many state data breach laws include private rights of action. California, Hawaii, Louisiana, and Washington include provisions in their laws that allow consumers to bring a civil action and recover damages.[65] The Federal Trade Commission and state attorneys general cannot pursue enforcement actions against every violation. A private right of action would empower consumers to enforce the law themselves and create a strong disincentive for the irresponsible handling of consumer data.

In addition, legislation should ban the use of arbitration clauses and class action waivers in consumer contracts. Consumers do not have the resources to pursue claims against powerful companies on their own. The Consumer Financial Protection Bureau ("CFPB") recently banned

---

[60] *"Cybersecurity and Data Protection in the Financial Services Sector," Hearing Before the H. Comm. on Fin. Servs.*, 112th Cong. (2011) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.

[61] *See* U.S. PIRG, *Security Freeze and Identity Theft Tips*, http://uspirg.org/sites/pirg/files/resources/Security%20Freeze%20and%20Identity%20Theft%20Tips.pdf.

[62] U.S. PIRG, *Interactive Map Shows Consumers in 42 States Have No Access to Free Credit Freezes* (Oct. 2, 2017), https://uspirg.org/news/usp/interactive-map-shows-consumers-42-states-have-no-access-free-credit-freezes.

[63] *Id.*

[64] *See*, The Privacy Act of 1974, 5 U.S.C. § 552a; Electronic Communications Privacy Act, 18 U.S.C § 2510 *et seq.*; Video Privacy Protection Act, 18 U.S.C. § 2710 *et seq.*; Telephone Consumer Protection Act, 47 U.S.C. § 227 *et seq.*

[65] Cal. Civ. Code 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 *et seq.* (2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).

arbitration clauses in consumer financial contracts, finding that class action waivers make it cost-prohibitive for consumers to obtain meaningful relief.[66] However, Congress recently voted to repeal that rule.[67] Companies that collect and store sensitive consumer data are in the best position to prevent data breaches, and they should be held liable when they fail to adopt reasonable security measures.[68] A private right of action that permits class actions is necessary to hold companies accountable for their data security failures.

F. Mandate algorithmic transparency

Consumers face the specter of a "scored society" where they do not have access to the most basic information about how they are evaluated.[69] Data brokers now use secret algorithms to build profiles on every American citizen whether they have allowed their personal data to be collected or not.[70] These secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' insurance rates, or even deny people jobs.[71] Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[72] In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage.[73]

The use of algorithms can also have widespread discriminatory effects.[74] The Equal Credit Opportunity Act (ECOA) prohibits lenders from discriminating in credit decisions.[75] But studies have demonstrated that black and Latino communities have lower credit scores as a group than whites.[76] Current law does not allow consumers or regulators to evaluate these scores to determine whether they violate ECOA.[77] Although consumers have the right to request their credit scores, they do not have the right to know how this score is determined.[78]

---

[66] 12 C.F.R. 1040; Consumer Fin. Prot. Bureau, *CFPB Study Finds That Arbitration Agreements Limit Relief For Consumers* (Mar. 10, 2015) https://www.consumerfinance.gov/about-us/newsroom/cfpb-study-finds-that-arbitration-agreements-limit-relief-for-consumers/.

[67] Donna Borak and Ted Barrett, *Senate Kills Rule That Made It Easier To Sue Banks*, CNN, (Oct. 25, 2017), https://www.cnn.com/2017/10/24/politics/senate-cfpb-arbitration-repeal/index.html.

[68] Brief of Amicus Curiae EPIC in Support of Appellants, *Storm v. Paytime*, No. 15-3690, at 25–30 (3d Cir. filed Apr. 18, 2016), https://epic.org/amicus/data-breach/storm/EPIC-Amicus-Storm-Paytime.pdf.

[69] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

[70] *Id.*

[71] *Exploring the Fintech Landscape: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. 7 (2017) (written testimony of Frank Pasquale, Professor of Law, University of Maryland).

[72] *Id.*

[73] Barry Ritholtz, Where's the Note? *Leads BAC to Ding Credit Score*, THE BIG PICTURE (Dec. 14, 2010), http://www.ritholtz.com/blog/2010/12/note-bac-credit-score/.

[74] *See, e.g.* Cathy O'Neil, *Weapons of Math Destruction* (2016); Danielle Keats Citron & Frank Pasquale, *The Scored Scoiety: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

[75] 15 U.S.C. § 1601 *et seq.*

[76] *See, e.g.* Consumer Fin. Prot. Bureau, *Analysis of Differences Between Consumer- and Creditor-Purchased Credit Scores*, (Sept. 18, 2012), http://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf.

[77] Citron & Pasquale, *supra*, note 72.

[78] 12 CFR Part 1002 ("Regulation B"); Citron & Pasquale, *supra*, note 54.

"Algorithmic transparency" is key to accountability.[79] Absent rules requiring the disclosure of these secret scores and the underlying data and algorithms upon which they are based, consumers will have no way to even know, let alone solve, these problems.

G. Provide Free Monitoring and Easy Access to Credit History

Current laws allow consumers to access free credit reports, but the process is cumbersome, and few consumers take advantage. A rationalized market would help ensure that consumers have as much information as possible about the use of their personal data by others. Instead, credit reporting agencies profit from the very problems they create. The Consumer Financial Protection Bureau also fined Equifax and TransUnion earlier this year after finding that the companies "lured consumers into costly recurring payments for credit-related products with false promises."[80] Credit reporting agencies should provide life-long credit monitoring services to consumers at no cost. Some credit card companies already offer similar services for free.[81] The other credit reporting agencies should do so as well.

H. Establish Federal Baselines Standards; Encourage States to Innovate as New Privacy Challenges Emerge

Today the states are on the front lines of consumer protection in the United States.[82] They are updating privacy laws to address new challenges.[83] They are bringing enforcement actions to safeguard American consumers.[84] They are establishing the data protection standards that are safeguarding the personal data of Americans from attack by foreign adversaries.[85]

It is absolutely essential to the development of privacy safeguards that Congress establishes baseline standards that all states must follow, but leave states with the freedom to adopt new protections. As Justice Brandeis once explained, the states are the laboratories of democracy.[86] This is all the more crucial in the rapidly evolving world of Internet services.

---

[79] EPIC, *Algorithmic Transparency,* https://epic.org/algorithmic-transparency/.
[80] Consumer Fin. Prot. Bureau, *CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products* (Jan. 3, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/.
[81] *See, e.g.*, Discover, *Social Security Alerts* (2017), https://www.discover.com/credit-cards/member-benefits/security/ssn-newaccount-alerts/.
[82] NCSL, *supra* at 57; EPIC, *State Policy Project*, https://www.epic.org/state-policy/.
[83] NCSL, *supra*, at 57.
[84] Fla. Att'y Gen., *Settlement Reached With Target Regarding Data Breach,* Press Release, (May 23, 2017), http://myfloridalegal.com/__852562220065EE67.nsf/0/267E8BE9BB21436C85258129005E37B8?Open&Highlight=0,data,breach; Reuters, *Washington state attorney general sues Uber after data breach*, (Nov. 28, 2017), https://www.reuters.com/article/us-uber-cyberattack/washington-state-attorney-general-sues-uber-after-data-breach-idUSKBN1DS2UF; N.Y. Att'y Gen., *A.G. Schneiderman Launches Formal Investigation Into Equifax Breach, Issues Consumer Alert,* Press Release, (Sep. 8, 2017), https://ag.ny.gov/press-release/ag-schneiderman-launches-formal-investigation-equifax-breach-issues-consumer-alert.
[85] EPIC, *State Consumer Data Security Policy*, https://epic.org/state-policy/consumer-data/.
[86] "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory[.]" *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (Brandeis, J. dissenting).

If Congress chooses to preempt the states in this crucial area of national security, it could leave Americans more vulnerable to attack from foreign adversaries.

IV. Congress should establish a data protection agency in the United States

The United States is one of the few democracies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the U.S. in the 1970s.[87] The United States was once a global leader on privacy. The Fair Credit Reporting Act, passed in 1970, was viewed at the time as the first modern privacy law—a response to the growing automation of personal data in the United States.[88] The Privacy Act of 1974 was based on the Code of Fair Information Practices, which have served as the foundation for international privacy laws and frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[89] and the European Commission's Data Protection Regulation.[90] This common approach to data protection helps facilitate international data transfer and trade.[91]

But today, Europe has surpassed the United States in protecting consumer data. The General Data Protection Regulation, which is set to take effect on May 25, 2018, strengthens the fundamental rights of individuals and puts consumers back in control of their personal data. It gives European data subjects rights to breach notification (within 72 hours of breach), right to access (whether or not personal data concerning them is being processed, where and for what purpose), right to be forgotten (to have the data controller erase his/her personal data, and data portability (the right for a data subject to receive the personal data concerning them and to transmit that data to another controller). American data subjects have none of these rights. American companies will be required to provide these protections to Europeans but not to Americans, creating a digital lower class. U.S. companies are leaders in technology, and the U.S. government should be a leader in technology policy.

There is an urgent need for leadership from the United States on data protection. Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges. The Federal Trade Commission is fundamentally not a data security agency. The FTC only has authority to bring enforcement actions against unfair and deceptive practices in the marketplace, and it lacks the ability to create prospective rules for data security. The Consumer Financial Protection Bureau similarly lacks

---

[87] See, EPIC, The Privacy Act of 1974, https://epic.org/privacy/1974act/#history.
[88] EPIC, *The Fair Credit Reporting Act*, https://www.epic.org/privacy/fcra/.
[89] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[90] Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), E.C. COM (2012) final, (Jan. 25, 2012), available at http://ec.europa/eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
[91] Marc Rotenberg, *In Support of a Data Protection Board in the United States, Government Information Quarterly*, vol. 8, no. 1, 79-94 (Spring 1991)

data protection authority and only has jurisdiction over financial institutions. Neither of these agencies possesses the expertise and resources needed to address data security across the country. And the Privacy and Civil Liberties Oversight Board, another agency that could help safeguard Americans and their data, lies dormant.

As the data breach epidemic reaches unprecedented levels, the need for an effective, independent data protection agency has never been greater. An independent agency can more effectively utilize its resources to police the current widespread exploitation of consumers' personal information. An independent agency would also be staffed with personnel who possess the requisite expertise to regulate the field of data security.

V. Current Legislative Proposals

There are bills in both the House and Senate that move in the right direction, but none are comprehensive data protection legislation. Data breaches affect all industries; therefore legislation that only applies to the credit bureaus will only address a small fraction of the problem. The Consumer Privacy Protection Act of 2017 (S. 2124), sponsored by Senator Patrick Leahy, is the most comprehensive proposal. It incorporates many of our suggestions including free credit freezes, objective data security standards, and a federal baseline.

The Comprehensive Consumer Credit Reporting Reform Act of 2017, (H.R. 3755), sponsored by Representative Maxine Waters, also includes several proposals we support. It expands consumers' access to free credit reports and limits the circumstances in which a credit reporting agency may furnish a consumer report for employment purposes. The bill also provides free credit freezes and credit monitoring for victims of identity theft, and caps the cost to place or lift a credit freeze at $3 for all other consumers.

Several bills propose amendments to FCRA. The PROTECT Act of 2017 (H.R. 4028 and S. 1982), sponsored by Representative Patrick McHenry and Senator David Purdue respectively, provides for federal supervision and examinations of the cybersecurity standards of large consumer reporting agencies. The bill also prohibits the use of SSNs by credit bureaus, and while this would be an improvement on the status quo, it would only limit the collection and use of the SSN by a few companies.

The Free Credit Freeze Act (H.R. 3878) prohibits bureaus from charging for placing, thawing, or lifting a credit freeze. But some proposals still allow bureaus to charge (e.g., H.R. 3755) and none require default freezes The Credit Information Protection Act of 2017 (H.R. 3766) only requires bureaus to provide free freezes after a breach has occurred. These bills contain some good measures, but they only marginally improve the regulatory landscape.

Some bills—including the Personal Data Notification and Protection Act of 2017 (H.R. 3806)—preempt state law. Data security is a dynamic field, so it is critical to ensure that the states are able to protect consumers. These bills should be modified to establish a federal baseline and allow states to regulate upwards, providing more protection than federal law if their legislatures so decide.

The Data Breach Prevention and Compensation Act of 2018 (S. 2289), sponsored by Senator Elizabeth Warren, comes close to creating a data protection authority by giving the FTC rulemaking authority. This would allow the agency to promulgate regulations setting standards for cybersecurity, setting clear standards that companies must meet.

The Data Broker Accountability and Transparency Act (S. 1815), sponsored by Senator Edward Markey, would address data protection beyond the credit reporting industry. S. 1815 applies to data brokers, including but not limited to credit bureaus, that collect and sell personal information to third parties. There are thousands of data brokers that make dossiers on individuals but are not regulated under FCRA because they do not create credit reports.

It is worth noting that members of both parties have introduced significant privacy bills in the House and the Senate. To be sure there is a lot of disagreement in Washington today. But on the issue of protecting the personal data of Americans, there is little reason for partisan disagreement. Privacy is an American value, and privacy protection is a fundamental American right.

Conclusion

EPIC believes it is time to enact comprehensive data protection legislation in the United States to and to establish a data protection agency. Our privacy laws are out of date and fail to provide the necessary protections for our modern age. We also face threats from foreign adversaries that target the personal data stored in U.S. companies and government agencies. The longer Congress delays, the greater the risks will be. Now is the time to act.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

Credit Union National Association
CUNA

WASHINGTON, D.C.
601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601
Phone: 202-638-5777
Fax: 202-638-7734

TESTIMONY

OF

KIM M. SPONEM
PRESIDENT & CEO
SUMMIT CREDIT UNION

BEFORE THE

FINANCIAL SERVICES SUBCOMMITEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"EXAMINING THE CURRENT DATA SECURITY AND
BREACH NOTIFICATION REGULATORY REGIME"

FEBRUARY 14, 2018

Testimony
of
Kim M. Sponem
President & CEO
Summit Credit Union
Before The
Financial Services Subcommittee on Financial Institutions and Consumer Credit
United States House of Representatives
At a Hearing Entitled,
"Examining the Current Data Security and Breach Notification Regulatory Regime"
February 14, 2018

Chairman Luetkemeyer, Ranking Member Clay, Members of the Subcommittee:

Thank you for the opportunity to testify on this extremely important topic. My name is Kim Sponem and I am CEO and President of Summit Credit Union, headquartered in Madison, Wisconsin. I serve as an ex-officio member of the Credit Union National Association (CUNA) Advocacy Committee on whose behalf I am testifying today.

Summit Credit Union is a state chartered credit union founded in 1935. We serve over 171,000 members and have over $2.9 billion in assets. We would be considered a large credit union. Credit unions range in size from nearly $80 billion in assets to less than $1 million in assets with most being small. In fact, of the nearly 6,000 credit unions in the United States half have less than $30 million in assets and fewer than eight employees, while twenty-five percent have less than $9 million in assets and fewer than three employees. More than 110 million Americans trust credit unions to provide them critical financial services with small credit unions often being the only option for financial services for many Americans. Summit Credit Union offers a full array of financial services to meet the needs of our members. As part of these services, Summit Credit Union offers debit and credit cards to allow our members to purchase goods and services almost anywhere.

Breach Impact on Summit Credit Union and Its Members

Unfortunately, merchant data breaches occur far too often and the cost to Summit Credit Union to cancel and reissue debit and credit cards continues to rise. For example, each year, we receive lists of debit and credit cards that were reported as compromised because of some type of

data breach. These lists could range from one card to many thousands of cards. Summit Credit Union follows specific procedures when notified of a data breach. Staff reviews the listed card numbers as the first step in determining the risk. Staff then decides if the credit union will block and reissue cards or tag the compromised card for additional fraud monitoring. In some cases, the card numbers we receive have already been reported to us (by the member) with fraud on them.

We have been harmed by data breaches occurring at large national merchants such as Target, Home Depot and Equifax as well as at small, local Wisconsin merchants that fail to take necessary steps to protect customer data. For example, in 2016 there was a local card processor that suffered a data breach. This processor routed transactions for a number of restaurants in the Madison area and surrounding communities. During a 4-month period we saw a large spike in fraudulent transactions with our members' credit and debit cards and identified that the common points of purchase were the restaurants that were using the breached processor. However, because we were not notified by this processor that it had been breached, we were required to reissue new credit and debit cards to these members as many as four separate times.

In 2017 alone, we reissued thousands of cards and incurred hundreds of thousands of dollars in losses from card fraud resulting from data breaches. These losses do not include the cost to reissue debit and credit cards or the number of staff hours spent on dealing with our customers' issues with respect to these data breaches. Some of the specific costs my credit union incurs when a data breach occurs at a merchant or processor include:

- Replacing debit and credit cards, which now include EMV or smart chips, the cost of which averages between $3.00 and $5.00 per card;
- Fraud monitoring, which is expensive and labor intensive;
- Addressing member calls and inquires;
- Processing and refunding fraudulent charges; and
- Processing compromised card reissuances.

Additionally, all members whose cards are breached are extremely inconvenienced when they:

- Have to report the fraud and have a new card reissued;
- Have their cards blocked by fraud monitoring so that the member's card is denied when attempting to make a purchase;

- Suffer added stress of knowing fraudsters possess their personal information;
- No longer have access to the use of their credit card when traveling due to it being blocked for fraud;
- Have their debit transactions declined for valid purchases if the fraudster has drained their account; and
- Have to update their automated payments every time their credit card is reissued. We have had several instances where a member forgot to update an automated payment with their new card information and suffered various consequences as the result of late payment.

Recently, we have seen a spike in identity theft. There have been several attempts at loan fraud where fraudsters are using other identities to attempt to obtain loans and open new accounts, which has also increased our costs.

We encourage our members to protect their data by putting a freeze or lock on their credit at the three credit bureaus; however, this takes action on behalf of the member every time they apply for credit and in some cases members incur a cost of $20 to $30 to unlock and relock access to their credit data. This also slows down the loan process and increases costs.

If a member is a victim of identity theft, it takes up a tremendous amount of staff resources to help the member navigate through the process of recovering their identity and rehabilitating their credit history.

We have invested in enhanced procedures in our remote contact areas to identify potential fraudulent activity, both when we review loan and new member applications, as well as with members calling in to conduct business on their accounts. We have also taken active steps to increase education and awareness for our members regarding the potential for card fraud or identity theft. These steps have increased costs to Summit Credit Union in the form of additional staff time to address fraud and support our customers.

Financial institutions, like Summit Credit Union, foot the bill for the fallout and subsequent fraud that comes from the breach of personal information from merchants and other companies' failure to adequately protect and secure customer information. The current state of the law does not put enough responsibility on those handing this sensitive customer information

to properly safeguarding it. Any future legislation must address this lack of responsibility and accountability.

Current Data Breach Landscape

Summit Credit Union is no different than any other financial institution when it comes to the impact it suffers when a data breach occurs. According to the Identity Theft Resource Center, the number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, which is an increase of 44.7 percent over 2016's record high. An annual fraud and risk survey from Kroll's found that in 2017, data theft has surpassed the theft of physical assets.

Without enhanced data security protections for all entities involved in the payments process we are likely to see no slowdown in data breaches in the following years.

Existing Data Security Requirements for Financial Institutions

Title V of the Gramm-Leach-Bliley Act (GLBA) subjects credit unions and banks to data security requirements. GLBA requires financial institutions to develop and maintain procedures and systems to protect consumer information from theft. Breach notification is also part of the GLBA requirements, which require credit unions and banks to notify members and consumers in the event of a breach. Merchants are not subject to similar requirements at the Federal level and the existing state laws do not do enough to protect consumers

Financial institution regulators have promulgated regulations to implement the GLBA requirements. The regulators also supervise financial institutions' compliance with GLBA requirements along with reviewing overall information technology programs for proper data security practices. Credit unions must comply with GLBA and be examined for compliance by a regulator- even the smallest credit unions with one employee.

Credit unions' experience with data security regulations clearly demonstrates that the smallest of businesses can comply with data security and notification requirements and that federal data security requirements would not be too burdensome for small merchants and other businesses. If credit unions and banks of all sizes are required to maintain strong procedures and systems, then merchants and other entities who access and obtain this data should likewise be held to similar standards regardless of size and sophistication.

Strong National Data Security Standard

Americans deserve a strong national data security standard that requires all businesses to protect and safeguard sensitive personal information. Credit unions and their customers will continue to unfairly and unnecessarily incur losses resulting from future data breaches if data security standards are not improved.

As I mentioned above, GLBA provides for requirements that protect members of the smallest to the largest credit unions while allowing these credit unions to operate efficiently. I know that there is concern that small businesses might have difficulty complying with a national data security standard, however small credit unions' ability to comply with the GLBA requirements demonstrates that the smallest businesses can successfully meet data security standards that are properly scaled to their size and risk level. It is important to remember that small businesses purchase credit card processing capabilities from vendors and that these vendors store most of the sensitive data for small businesses. It would seem that these businesses and vendors should be able to bear the responsibility for data security compliance like credit unions do already.

A national data security standard would simplify compliance and notification requirements for businesses. The majority of states and territories have enacted laws governing data security or breach notification. While this patchwork of laws provides some protection for consumers, the differences highlight the need for a baseline national standard. A national standard would ensure that all consumers and financial institutions are protected at least at some level, without preempting any states' right to impose additional requirements.

Strong Notification Requirements

Consumers have the right to know when their personal information has been stolen or lost from a breach or by other means. There is no current federal law that requires merchants or the many others that possess or handle such information to notify consumers or financial institutions when a breach has occurred or within any standard timeframe. Because of the lack of a uniform notification requirement, consumers are often unaware a data breach has occurred and may never learn that their personal information has been stolen or lost. Often, consumers first learn that their personal information has been compromised when their financial institution replaces their debit or credit card. Indeed, many times credit unions like my credit union do not learn of a data

breach until a card processor or card brand notifies us that a breach may have occurred or is covered in the media. This can sometimes be too late to protect the credit union and its members from fraud.

Expedient notification of all stakeholders is a simple and cost-effective way to add a layer of protection to those whose data has been lost and other important stakeholders in the payments ecosystem. It allows consumers and other stakeholders the ability to mitigate possible losses or to address other issues related to a breach. Furthermore, notification also gives consumers the information necessary to protect themselves and enables them to decide whether to keep doing business with a breached entity.

Prompt and uniform consumer notification also assists financial institutions with respect to payment card replacement. Although there are no specific requirements that prevent a credit union from notifying members that a breach has occurred, most may be hesitant to do this because information often is incomplete after a breach. Merchants and other entities that possess payment card and other personal information should take responsibility for their systems and ensure that consumers and other stakeholders are properly notified when a data breach occurs, just as financial institutions are required to do.

Shared Responsibility Costs

CUNA and a number of credit unions, including my credit union, have filed lawsuits to protect other credit unions and their members from harm resulting from the Equifax data breach. The Equifax data breach has harmed and will continue to harm Summit Credit Union, other credit unions, and their members. Hackers had access to highly sensitive personal information and payment card data for months, exposing credit unions to damages in replacing members' payment cards, covering fraudulent purchases, and taking protective measures to reduce the increased risk of identity theft and loan fraud. Credit unions are required to assume financial responsibility for various types of fraudulent activity related to stolen identities and misuse of personal information and payment card data. As the Wall Street Journal just reported on Friday, Equifax submitted a report to the Senate Banking Committee indicating that hackers breached even more information than previously reported, including additional driver's licenses, Tax ID numbers, and email addresses. The lack of any effective data security standards allowed Equifax to ignore the numerous entities who issued public warnings in March 2017 regarding the Apache

Struts vulnerability. Equifax did not update this software to its latest version. In a statement posted September 14, 2017, the Apache Software Foundation attributed the Equifax data breach to Equifax's failure to update this software. Equifax should be held accountable. Any institution that either fails or consciously decides not to implement adequate data security measures should be held accountable to those that they have harmed.

Summit Credit Union is suing Equifax to recover costs and losses directly resulting from the data breach for itself and other credit unions and financial institutions throughout the United States. We also seek to have Equifax take the necessary steps to enhance its current data security to prevent a future breach from occurring. We believe that any business or other entity that possesses or handles consumers' data should be responsible for damage to others resulting from a breach or other loss of this data. My credit union carefully considered litigation as a means to recover from Equifax. Litigation is currently the best way to recover losses stemming from a data breach, and a national standard to hold those entities accountable is warranted.

My credit union and other credit unions need data breach legislation that makes the breached entity responsible to others in the payments ecosystem for losses and other damages that are the result of a data breach. The current system where consumers are protected from loss because financial institutions bear the responsibility for reimbursing their members and customers for losses stemming from data breaches is not fair or sustainable, as the pace and losses from breaches accelerate year after year. Thus, under the current system, financial institutions essentially provide insurance for the entire payments ecosystem while those merchants and other entities whose deficient systems cause the breach, have little incentive to properly safeguard consumers' data because they have no financial incentive or legal requirement to do so.

All participants in the payments ecosystem should be subject to data security requirements and all participants should bear the costs to others from a breach of their system. Properly allocating costs and requirements will cause companies to take action to improve their systems. Enhanced data security requirements will ensure that there is shared responsibility for securing information and costs.

We recognize that data security should be one of the priorities for 2018 and that enhancing payment security to reduce the impact that merchant data breaches have on credit unions and their members is a goal of any proposed legislation. We support strong data security

and data breach notification requirements and will work with policymakers to strengthen the cyber infrastructure to protect consumer data from attack and hold accountable those that fail to adequately protect this information.

On behalf of America's credit unions and their 110 million members, thank you for the opportunity to testify today. I am happy to answer any questions the Subcommittee may have.

Additional Examples of How Breaches Impact Summit Credit Union Members

In addition to the financial harm borne by credit unions and its customers resulting from a data breach, our customers also face significant issues arising from these data breaches. For example, I worked with one member who sent her daughter abroad to study. Her daughter's card was affected by a breach and had fraudulent charges coming through so it was closed. Her daughter was stranded in another country without access to her money. The mother was quite distraught, as you can imagine. She had an email from her daughter but was unable to reach her by phone or text. Imagine having your child stranded with no access to money in a foreign country and almost no way to communicate with her.

We spent a great deal of time coordinating efforts, and we were finally able to send funds via Western Union, communicating with mom and daughter via e-mail.

We had one member who was an over the road truck driver. He was down south and went to fill up his truck and was denied at the pump. He called in a panic as he had a timeline to meet. We did some research for him and found a credit union shared service center a few miles away. He had to drive his semi there, find a place to leave it so he could go in and make a withdrawal. His card had been compromised in a breach, and when fraud occurred his card was shut down.

Another member called in because her daughter's card was involved in a breach and her payment card was shut down for fraud. The mother was furious as the daughter was away at college and had no money to buy food. Her debit card was all she had. As a result of this situation, we rush ordered a card at our expense ($50) to get her daughter a new card the next day. None of these costs are borne by the entities that caused these breaches.

We have had several members who have had their cards blocked while overseas traveling. Sometimes people do not take more than one way to access money when traveling. On more than one occasion we have received emails from members who are panicked as to what to do. We have actually overnighted (again, at our expense) new cards to hotels in other countries. And on at least one occasion, we wired funds to the hotel to pay the hotel bill for a member who could not check out.

Finally, there was a member who was auto-paying her rent with her credit card. When her card was shut down, she forgot to notify her landlord of her new credit card number. When her rent payment was charged to her now-canceled credit card account and rejected, the landlord

notified her that they would only accept a money order going forward. We talked to the landlord and then sent a letter explaining that this was not her fault, she had been a victim of a credit card breach. We were able to get her back in good graces with her landlord.

When a breach occurs, many members want to cancel cards and have new ones reissued because they are so afraid of having fraud occur on their card. They do not understand how this type of fraud can happen, as they have chip cards. They expect their financial institution to protect them from fraud and are angry that their information has been compromised. However, they do not understand that their financial institution had nothing to do with their information being compromised.

TESTIMONY OF

NATHAN TAYLOR

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

EXAMINING THE CURRENT DATA SECURITY AND BREACH NOTIFICATION REGULATORY REGIME

FEBRUARY 14, 2018

Chairman Luetkemeyer, Ranking Member Clay and members of the Subcommittee, my name is Nathan Taylor, and I am a partner at the law firm of Morrison & Foerster LLP in the firm's Financial Services and Privacy and Data Security practice groups. My practice is focused on helping financial institutions and other companies (*e.g.*, retailers and technology companies) protect the security of sensitive information and respond to the unfortunate security incidents involving that information that inevitably occur. My colleagues and I have represented companies in responding to a number of the largest and highest-profile data breaches in American history. I am pleased to be here today to provide background on the current legal landscape of state "safeguards" laws and breach notification laws, as well as to discuss some of the challenges that companies face in responding to security incidents.

At the outset, I would like to stress that I share your concerns about the critical need to protect American consumers and businesses from the constantly evolving and increasingly sophisticated cybersecurity threats that exist today. Although the word "cybersecurity" was not used in the English language until the late 1980s, it has rapidly become one of the most critical issues for our nation and society. Cybersecurity impacts not only the security of our own sensitive personal information, but also the security of our government, our critical infrastructure, our technology, our national defense, our elections and, in the increasingly Internet-connected world, our way of life.

Congress, including this Committee, has considered the issue of data security and breach notification for 15 years. *See, e.g.*, H.R. 3997, Data Accountability and Trust Act (introduced Oct. 6, 2005), *available at* https://www.congress.gov/bill/109th-congress/house-bill/3997. It goes without saying that during that time the issue of cybersecurity has grown ever more critical. Today, the obligation (if any) under state law to protect sensitive personal information about you depends entirely on where you live. That is, whether there is a state requirement to protect, for example, your Social Security number and financial account information is dictated by the state in which you reside. In addition, even though most states have enacted security breach notification laws, these laws often contain conflicting provisions, which complicates the process of responding to security breaches. Simply put, we need a single, nationwide standard to address what is truly a national issue.

I strongly believe that a single, nationwide standard for data security and breach notification would be good for both American consumers and American businesses. American consumers would benefit if all companies that may handle sensitive personal information about them are subject to the same strong federal standards to protect that information and to provide them with timely notice in the event of a security incident involving that information. American businesses would benefit from being able consistently to apply a single standard to protect sensitive personal information and to respond to the unfortunate, but inevitable, security incidents involving that information. I believe the time for Congress to act on this important issue is now.

Overview of State Safeguards and Security Breach Notification Laws

In order to advise companies on compliance with state law, it is critical to my practice that I have a deep understanding of the various state "safeguards" laws and breach notification laws, as well as related developments in state legislatures around the country. For more than a

decade, I have tracked each new state safeguards law and breach notification law and the many amendments to those laws that have followed. When you review the landscape of state laws that exist today, you find a complex matrix of inconsistent, sometimes duplicative and often contradictory requirements. In my testimony, I will focus on providing an overview of these state laws, including providing examples of how the state laws are either inconsistent or contradict in ways that result in consumers being treated differently based on where in the United States they live.

State Safeguards Laws

As discussed below, only two states have yet to enact breach notification laws. The opposite is true with respect to state requirements to protect information about consumers. Few states impose general obligations on companies to protect sensitive personal information.[1] As a result, whether there is a state obligation to protect sensitive information about a consumer, such as Social Security number or payment card information, depends entirely on the consumer's state of residence. And, more specifically, unless the consumer lives in one of several states, most businesses that handle sensitive information about the consumer are not subject to a state requirement to protect that information.

State Safeguards Laws

Only 15 states impose general requirements that businesses must protect sensitive personal information. Most of these state safeguards laws impose only high-level security obligations, typically a general obligation to take reasonable steps to secure data or to maintain reasonable security controls to protect data. For example, the California safeguards law provides that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b). These safeguards laws also typically include obligations for the secure disposal of information.

It is important to note that several of these 15 states do, in fact, have detailed safeguards laws that include specific security requirements, often modeled, at least in part, on the safeguards rule issued by the Federal Trade Commission pursuant to Section 501(b) of the Gramm-Leach-Bliley Act. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436–1437 (1999); 16 C.F.R. pt. 314. For example, the Massachusetts data security rules and the Oregon safeguards law contain detailed safeguards provisions, including requirements to maintain risk-based information security programs that include safeguards designed to protect sensitive personal information against cybersecurity risks, to designate an individual to be responsible for overseeing and appropriately to oversee services providers who will have access to sensitive information. *See* 201 Mass. Code Regs. § 17.03; Or. Rev. Stat. § 646A.622. The Massachusetts data security rules and the Nevada safeguards law also include technology-specific requirements, such as

[1] The following discussion addresses state safeguards and disposal laws that apply to any business handling sensitive information relating to residents of the relevant states. It does not address state requirements that apply only to specific sectors, such as the financial sector. *See, e.g.*, N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.0 – 500.23 (rules for financial institutions subject to the authority of the New York Department of Financial Services); N.J. Stat. §§ 56:8-196 – 56:8-198 (security requirements for health insurance carriers).

requiring the encryption of data that is maintained on certain devices (*e.g.*, laptops) or that is transmitted electronically in certain ways (*e.g.*, over the Internet). 201 Mass. Code Regs. §§ 17.04(3), (5); Nev. Rev. Stat. § 603A.215(2).

In contrast, 35 states impose no obligation for companies to protect sensitive personal information, other than the secure disposal of information noted below.

State Disposal Laws

Although having a far narrower focus, 17 states, in addition to those noted above, have enacted laws that require the secure disposal of sensitive personal information that a business will no longer retain. For example, the Arizona disposal law prohibits a person from "knowingly discard[ing] or dispos[ing] of records or documents without redacting the information or destroying the records or documents if the records or documents contain" sensitive personal information. Ariz. Rev. Stat. § 44-7601(A). These state disposal laws, however, do not impose any obligation to protect the security of information *before* it will no longer be retained.

The Importance of a Single, National Standard for Data Security

If you are an American, where you live should not dictate whether there is a legal obligation to protect sensitive personal information about you. In my view, this point is not controversial. Most people would agree that a consumer's Social Security number and financial account information, among other things, are sensitive and, if in the wrong hands, could be misused in ways that cause the consumer harm. The sensitivity of this information and the related risks associated with its misuse are the same for all Americans, regardless of where they live.

Today, however, only a small minority of states impose substantive security requirements for the protection of sensitive personal information. While it is true that for many companies operating on a nationwide basis, the few detailed state safeguards laws (*e.g.*, the Massachusetts data security rules) often become the *de facto* national standard. That is, companies operating on a nationwide basis often develop a single compliance strategy that attempts to incorporate the security requirements of all applicable state safeguards laws. However, practical considerations typically drive that result, not the law. And, companies that maintain information on consumers in just a few states may not be subject to any substantive state security requirements at all.

In my view, this is not an equitable or appropriate result. Regardless of whether a consumer lives in, for example, Walnut Creek, California, Nampa, Idaho, Abilene, Texas or Norristown, Pennsylvania, sensitive personal information about the consumer should be protected. A single, national standard for security would accomplish that result, to the good of all Americans. This would also benefit American businesses by leveling the playing field to ensure that all companies are subject to robust requirements, while simplifying the compliance process so that a company can focus on a single federal law as opposed to disparate and often inconsistent state laws.

Overview of State Breach Notification Laws

To date, 48 states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted breach notification laws.[2] These laws ostensibly share the same purpose—ensuring that consumers receive notice of security incidents involving sensitive personal information about them so they can take steps to protect themselves from harm. In this regard, each state law's consumer notification trigger is based, at least in part, on some form of unauthorized, unlawful or illegal access to, or acquisition or use of, certain types of sensitive personal information.

Nonetheless, these state laws are far from uniform. In fact, they vary significantly in terms of their requirements, including scope, the types of personal information covered, notice content requirements and related obligations. These inconsistencies can lead to results that are unfair to consumers and unduly burdensome to businesses. If multiple companies experience the same type of breach involving the same exact facts except that the information involved in the different breaches relates to residents of different states, some consumers may receive notice, while others may not. And for those receiving notice, the notices may include different content and be provided in different forms at different times.

To give a sense of the ways in which the 52 breach notification laws can be inconsistent and/or conflict, the following provides a high-level discussion of two aspects of state breach notification laws: (1) requirements for the content of a consumer breach notice; and (2) notification requirements for incidents involving electronic/computerized data vs. data in paper form. There are many other meaningful differences that I could discuss, but the following are illustrative.

Content Requirements for a Consumer Breach Notice

Of the 52 laws, only 22 impose requirements for what the consumer must be told about the incident (*i.e.*, the types of information that must be included in a breach notice).[3] The notice content requirements typically focus on providing consumers with information about the nature of the incident, the types of information involved in the incident and steps consumers can take to protect themselves from harm. For example, the West Virginia law requires that a breach notice include a description of the types of information that were involved in the incident, a telephone number or website that the individual can use to contact the entity that experienced the breach and learn more about the incident, information on how a consumer can place a security freeze or fraud alert and toll-free telephone numbers and addresses for the major consumer reporting agencies. W.V. Code § 46A-2A-102(d)(1).

Some states require that a breach notice include information that is uniquely specific to residents of those states, such as contact information for state government entities. For example, the North Carolina law requires that a breach notice include "[t]he toll-free numbers, addresses,

[2] The following discussion addresses state breach notification laws that apply to any business handling sensitive information relating to residents of the relevant states. It does not address state breach notification requirements that apply only to specific sectors, such as health insurers. *See, e.g.*, Conn. Gen. Stat § 38a-999b.

[3] Two states impose requirements for the content of certain, but not all, breach notices. *See, e.g.*, 73 Penn. Stat. § 2302 (providing standards for the content of a telephonic notice).

and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft." N.C. Gen. Stat. § 75-65(d)(7). Although there often are significant differences from state to state in terms of the specific content required in a breach notice, the most common content requirement is that a breach notice must include a basic description of the incident. *See, e.g.*, Haw. Rev. Stat. §§ 487N-2(d)(1).

Some states go beyond the content of the notice and impose requirements for how that content must be presented, such as requiring that a notice be clear and conspicuous. *See, e.g.*, Mich. Comp. Laws § 445.72(6)(a) (requiring notice to "be written in a clear and conspicuous manner"). For example, the California law requires, among other things, that a notice "be written in plain language," include a specific title (*i.e.*, "Notice of Data Breach"), include specific headings (*e.g.*, "What Happened") and be written in "no smaller than 10-point type." Cal. Civ. Code § 1798.82(d)(1).

Although the state laws are far from consistent with respect to the required content for a breach notice, the Massachusetts law provides the most dramatic example of how state breach laws can conflict in material ways that complicate the process of responding to a breach. Specifically, the Massachusetts law *prohibits* a business from including in a breach notice "the nature of the breach or unauthorized acquisition or use." Mass. Gen. Laws § 93H-3(b). That is, a business that is required to provide notice to a Massachusetts resident about a breach involving sensitive information relating to the individual *may not* tell the individual basic information about the incident. As discussed below, while the Massachusetts content prohibition may be viewed as an outlier, it nonetheless complicates how companies respond to "nationwide" breaches.

Computer vs. Paper Breaches

Of the 52 laws, 43 apply only with respect to breaches involving computerized or electronic data that contains sensitive personal information. *See, e.g.*, Va. Code § 18.2-186.6 (defining a breach, in pertinent part, as "the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information"). The remaining nine state laws apply with respect to different forms of data beyond computerized data.

For example, the Alaska, Hawaii, Massachusetts, North Carolina and Washington laws apply with respect to breaches of sensitive personal information in any form. *See, e.g.*, N.C. Gen. Stat. § 75-65(a) (requiring notification regarding breaches involving "personal information in any form (whether computerized, paper, or otherwise)"). The Rhode Island law applies with respect to breaches involving personal information in computerized or paper form. R.I. Gen. Laws § 11-49.3-3(a)(8) (defining "personal information," in pertinent part, as unencrypted data and data "in hard copy, paper format"). The Indiana and Iowa laws are unique in that they apply to breaches involving computerized data and computerized data that have been transferred to another medium, such as paper. Ind. Code § 24-4.9-2-2(a); Iowa Code § 715C.1(1). Finally, the Wisconsin law is simply silent as to the form of data covered by the statute. *See* Wis. Stat. § 134.98.

Practical Challenges in Responding to a Breach

In the context of discussing the requirements of state breach notification laws, it is important to note some of the practical challenges that a company can face in responding to a significant breach, particularly one involving some type of computer or electronic intrusion. Even for companies who respond diligently and expeditiously, all the steps involved in investigating the incident, restoring the security of systems and preparing the response take time.

It is critical to highlight that a company's first indication of a breach (with the benefit of hindsight) is often fairly innocuous. At that time, the company may not realize that it is under attack. In my practice, I have seen many incidents that "begin" with an anomalous fact that is not itself indicia of a breach, such as, for example, a company receiving an IT alert that the performance of a server has slowed or that a server is nearing its storage capacity. And there are instances where the attackers feint to distract the company with a "decoy" attack, such as ransomware or a denial of service attack that requires a response from the company, but is not the ultimate goal of the attacker. Of course, there are also incidents where the first fact that the company learns creates a strong suspicion that data has been stolen, such, as for example, a call from the Federal Bureau of Investigation informing the company that information related to the company has been found online or on devices seized by law enforcement (*e.g.*, for sale on the "dark web").

Even when a company believes that an attacker has likely penetrated its defenses, the company has to investigate to determine the scope and extent of the breach, including, for example, determining whether data was actually stolen (which is not always the case). The resulting forensic investigation must attempt to recreate the attacker's steps to determine, among other things, what systems, applications and databases were accessed by the attacker, what commands were run, what changes were made and what data was stolen. This process grows more complex when the attacker has had prolonged access to systems or when the impacted systems are vast. While confirming the basic facts of what happened may seem simple in principle, it involves a detailed forensic review and analysis combing through logs, artifacts and other evidence, much like trying to recreate a crime scene.

Separate and apart from any steps that a company may take to determine whether consumer data has been stolen, the most important aspect of a company's initial response to a breach is its efforts to ensure that the attacker has been removed from its systems, as well as to address and remediate any issues or vulnerabilities that were exploited by the attacker in the first instance. This need becomes even more immediate when the breach will become public, thereby making the company a target for other attackers.

Even where a company believes that data has been stolen, it is often difficult to determine the exact data elements involved and the consumers to whom that information relates. For example, attackers often exfiltrate data from a company's systems in a highly encrypted format. As a result, the effort to confirm which data was stolen often involves a process of recreating the attacker's searches to determine the types of data the attacker likely accessed. This is often complicated by the fact that a company is recreating the attacker's steps at a later point in time, after the underlying data set has changed. Regardless, this is a critical step that companies take very seriously because the ramifications are significant. Specifically, a company needs to be

able to determine the specific data stolen so that it can ensure that the right consumers are notified. A company does not want to incorrectly notify a consumer that her data was lost and create unwarranted concern or confusion when the consumer is actually not at risk.

When a company determines that notice to consumers is required or otherwise appropriate, its work is only beginning. Particularly for large breaches, there are a number of critical steps that a company must take in order to provide notice to consumers. These steps include engaging third-party vendors (*e.g.*, a company to offer credit monitoring to consumers), preparing mailings (*e.g.*, validating mailing addresses, deduplicating the mailing list and printing letters and envelopes), preparing FAQs to be able to respond to consumer questions, setting up toll-free telephone numbers and arranging for sufficient call center capacity, to name just a few. This already complex process is made more difficult by the fact that a company must ensure that its various steps comply with the requirements of 52 different breach laws.

The Importance of a Single, National Standard for Breach Notification

Although virtually all states have breach notification laws, these laws contain many meaningful differences. These differences impact whether (if at all) a consumer receives a breach notice, what the breach notice says, when it is sent to the consumer and even how it is sent. In addition, the many differences complicate the process that a company must go through to respond to a breach involving sensitive information relating to Americans residing around the country or within multiple states.

Take, for example, the issue of the content of a breach notice discussed above. In providing notice to Americans throughout the country for a "nationwide" breach, a company can send a single notice to residents of all states other than Massachusetts and include in that notice all of the content required by the various states other than Massachusetts. The notice will often highlight certain content as being for residents of specific states, such as contact information for a state Attorney General. The company will then send a different and separate notice to residents of Massachusetts. This Massachusetts notice will omit any discussion of what happened to the consumer's information, as well as any content required by other states. Not only does this complicate the notification process, but it also has the adverse effect of ensuring that all Americans do not receive the same information about the same breach.

While many companies that experience "nationwide" breaches create strategies designed to treat all consumers equally from a notice standpoint regardless of where they live (to the extent permitted by law), this is not a requirement. For example, a company experiencing a nationwide breach could elect to comply with each of the 52 laws separately and develop state-specific notices based solely on each law's requirements (if any).

For every "nationwide" breach, however, there are thousands of breaches that involve information relating to residents of one state or several states. In this regard, for breaches involving sensitive information relating to residents of a single state (or several states), companies typically look to the law of that single state and craft their responses and consumer notices to comply with the relevant law. As a result, if two companies experience the same type of breach with the same facts and involving the same types of sensitive personal information, some consumers may receive notice, while others do not, solely because of where the consumers

live. And for those consumers who do receive notice, the consumers may receive different information, not because the facts may necessitate a different notice, but because the consumers live in a state that has no content requirements or the state's content requirements differ from those of other states.

Similar to my views on state safeguards laws, this is not an equitable or appropriate result. If a consumer's Social Security number is lost or stolen and the consumer is at risk of harm as a result of the incident, the consumer should receive notice, at the same time, in the same form and with the same content, regardless of whether he or she lives in, to use my earlier example, Walnut Creek, California, Nampa, Idaho, Abilene, Texas or Norristown, Pennsylvania. A single, nationwide standard for breach notification would accomplish that result. In the process, American businesses would benefit significantly. Specifically, a company would be able to craft a response strategy that is designed to comply with a single federal standard without having to address the nuances and inconsistencies of 52 different laws. This would allow companies to respond faster, to the benefit of the American consumer.

The Path Forward

I would like to reiterate my strong belief that a single, nationwide standard for data security and breach notification would be good for both American consumers and businesses. American consumers would benefit by receiving the same protections for sensitive personal information about them regardless of where they may live. American businesses would benefit from a single standard that can be applied consistently to protect sensitive personal information and to respond to the unfortunate, but inevitable, security incidents. This is a national issue, and I believe that the time is now for Congress to act.

With respect to drafting legislation to address this important issue, I believe any legislation that this Committee considers should, at a minimum, address the following four principles:

(1) A federal bill should include strong, yet flexible and scalable, data protection standards for all companies that handle sensitive personal information;

(2) A federal bill should require notification to consumers in the event of a breach that puts consumers at risk of harm;

(3) A federal bill should recognize existing federal standards on data security and breach notification, including under, for example, Title V of the Gramm-Leach-Bliley Act, and deem entities subject to those standards to be in compliance with the legislation if they comply with their existing federal obligations; and

(4) A federal bill should preempt state safeguards laws and breach notification laws to ensure that all Americans receive the same level of protection regardless of where they live.

* * * *

Thank you for the opportunity to speak with you today. I would be happy to address any questions that you may have.

February 13, 2018

The Honorable Blaine Luetkemeyer
Chairman
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
Washington, DC 20510

The Honorable Willliam Lacy Clay
Ranking Member
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
Washington, DC 20510

RE: Hearing on "Examining the Current Data Security And Breach Notification Regulatory Regime"

Dear Chairman Luetkemeyer and Ranking Member Lacy Clay,

The undersigned associations represent over a million businesses in industries that directly serve American consumers. Our organizations appreciate the Committee calling a hearing to examine the current data security and breach notification regulatory regime. Our members are committed to protecting their customers' data with effective data security practices and take the risk of breaches of security very seriously. In addition to the financial services companies under the Committee's jurisdiction and our members' businesses, the rampant nature of threats to consumer data is a challenge for businesses of all kinds. This includes companies that support communications with consumers and facilitate the acceptance of their forms of payment, as well as for professional organizations, health care institutions and government agencies.

Every industry sector – whether consumer-facing or business-to-business – suffers data security breaches that may put consumer data at risk. Less well known, however, is that three sectors in particular account for more than half of all breaches (i.e., security incidents with confirmed data losses) according to the 2017 Verizon Data Breach Investigations Report: financial services (24.3% of all breaches); healthcare (15.3%); and the public sector (e.g., governmental entities) (12.4%). According to this report, well above 80% of all breaches in 2016 occurred *outside* of the industries represented by the signatories to this letter, whose businesses typically handle less sensitive data than the sectors accounting for most breaches.

To protect consumers comprehensively, wherever breaches occur, Congress should ensure that any federal breach notification law applies to *all* affected industry sectors and leaves no holes in our system that would enable some industries to keep the fact of their breaches secret. Under the breach legislation reported by the House Financial Services Committee last Congress, however, Equifax would have been exempt from the bill's provisions along with banks, credit unions and other entities that qualify as "financial institutions" under the Gramm Leach Bliley Act (GLBA). The absence of breach notice requirements for entities accounting for roughly a quarter of all security breaches annually would have left millions of Americans unaware of their potential risks of financial harm and identity theft. The exemption of Equifax and other financial services companies from the requirements of that bill would have created particularly weak

public policy given that the same bill provided those companies with preemption from the requirements of state laws.

Considering the widespread risk of data breaches afflicting all American industries and our governmental institutions, there are four key principles we support in federal data security and breach notification legislation:

1. **Establish Uniform Nationwide Law**: First, with the fifty-two inconsistent breach laws currently in effect in 48 states and 4 federal jurisdictions, there is no sound reason to enact federal legislation in this area unless it preempts the existing laws to establish a uniform, nationwide standard so that every business and consumer knows the singular rules of the road. One 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. Simply enacting a different, fifty-third law on this subject would not advance data security or consumer notification; it would only create more confusion.

2. **Promote Reasonable Data Security Standards**: Second, data security requirements in a federal law applicable to a broad array of U.S. businesses should be based on a standard of reasonableness. America's commercial businesses are remarkably diverse in size, scope and operations. A reasonable standard, consistent with federal consumer protection laws applicable to businesses of all types and sizes, would allow the right degree of flexibility while giving businesses the appropriate level of guidance they need to comply. Legislation taking this approach also would be consistent with the data security standard now used by the Federal Trade Commission (FTC) and nearly all state laws that include data security requirements in their breach notification statutes.

3. **Maintain Appropriate FTC Enforcement Regime**: Third, federal agencies should not be granted overly-punitive enforcement authority that exceeds current legal frameworks. For example, absent a completed rulemaking, the FTC must bring an action requiring a business to stop behavior that the FTC deems to be a violation of law. The FTC cannot seek civil penalties until it establishes what a violation is. That process gives businesses notice of the FTC's view of the law and is fair given the breadth of the FTC's discretion to determine what is legal.

4. **Ensure All Breached Entities Have Notice Obligations**: Finally, businesses in every affected industry sector should have an obligation to notify consumers when they suffer a breach of sensitive personal information that creates a risk of identity theft or financial harm. Informing the public of breaches can help consumers take steps to protect themselves from potential harm. Moreover, the prospect of public disclosure of breaches creates greater incentives for all businesses handling sensitive personal information to improve their data security practices. Creating exemptions for

particular industry sectors or allowing breached entities to shift their notification burdens onto other businesses will weaken the effectiveness of the legislation, undermine consumer confidence, ignore the scope of the problem, and create loopholes that criminals can exploit.

We note that a group of organizations led by the Financial Services Roundtable (FSR) wrote to the House Energy and Commerce Committee on January 4, 2018, relaying the elements of legislation that those groups favor. The FSR letter advocated for a "flexible, scalable" data security standard that included factors such as the "size and complexity" of a business, the "cost of available tools to secure data," the "sensitivity" of the information the company maintains, and "guarantees" that small businesses are not excessively burdened. The reasonableness standard endorsed by the FTC that the undersigned organizations support already meets all of those criteria. However, as soon as laws mandate specific data security requirements for businesses, they become inflexible and burdensome for smaller entities, and outdated and inadequate for larger or more sophisticated businesses. We appreciate that the FSR-led letter appears to agree with us on this point.

We are also pleased that the FSR-led letter appears to agree with our principle on breach notification requirements for entities handling information that, if breached, may cause individuals to become victims of financial harm or identity theft. Their letter calls for a "notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators." In the past, this Committee's breach legislation has exempted businesses in industries such as telecommunications, financial services, and data storage from required consumer notice when they are breached. That certainly would not meet the language of the FSR-led letter and is not acceptable to our organizations either. While some businesses subject to GLBA have asked for exemptions from notice obligations in new legislation, those requests raise significant problems given that GLBA does not require breach notification.[1] No industries are exempt from the attention of data thieves and no industries should be exempt from a statutory requirement to provide notice to consumers when they have breaches. Legislation should not serve as cover for giving breached businesses the ability to keep secret their own breaches and the risks of harm to affected individuals.

The four principles above, which are supported by the undersigned organizations, are important to ensure that any data security and breach notification legislation advanced in Congress does not overly burden business already victimized by a breach, does not impose unfair burdens on unbreached entities, and does not pick regulatory winners and losers among differing business sectors in the process. We urge you to exercise your leadership to find legislation that can meet these four principles. Additionally, any such process needs to include input from all affected industries and from businesses of all sizes. Otherwise, it risks imposing unfair or

[1] GLBA's statutory language, approved by Congress in 1999, predates the first state breach notification law by several years and does not actually require notification of security breaches. Regulatory guidelines implementing GLBA adopted in 2005 recognized this omission, but did not correct it. Rather, the guidelines state that GLBA-covered entities *"should"* make breach notice, but notice is discretionary and not a *requirement*. Legislation exempting GLBA-covered entities therefore leaves them without a notice requirement.

crippling burdens on some sectors but not others, which, unfortunately, has been the case with several past legislative proposals.

We appreciate your consideration of our views as on this hearing and we look forward to a continued constructive dialogue with you on these matters.

Sincerely,

American Hotel & Lodging Association
International Franchise Association
National Association of Convenience Stores
National Association of Realtors
National Association of Truck Stop Operators
National Council of Chain Restaurants
National Grocers Association
National Restaurant Association
National Retail Federation
Society of Independent Gasoline Marketers of America
U.S. Travel Association

cc: Members of the U.S. House of Representatives

On behalf of the nearly 5,700 community banks represented by ICBA, we thank Chairman Luetkemeyer, Ranking Member Clay, and members of the Financial Services Subcommittee on Financial Institutions and Consumer Credit for convening today's hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime." ICBA is pleased to have the opportunity to offer this statement for the hearing record.

Community banks are committed to safeguarding customer data and personal information. The community bank business model is founded on customer trust and service. Data security is a business imperative in the digital marketplace. Community banks invest significant and increasing resources in security controls to protect their consumers' data and critical systems.

ICBA also urges Congress to be part of the data security solution by taking aggressive action as described below.

Examination and Supervision of Credit Reporting Agencies

The Equifax breach shows the ongoing vulnerability of credit reporting agencies (CRAs). While CRAs are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA), they are not examined or supervised for their compliance with these standards in the same manner as financial institutions, yet they hold equally critical, personally sensitive information about consumers. This is a grave weakness that must be addressed in any data security legislation. Significant third-party vendors that serve financial institutions are already subject to examination and supervision for compliance with GLBA standards. By the same logic, CRAs should be examined and supervised by the prudential financial regulators.

ICBA Lawsuit Against Equifax

ICBA and community bankers were appalled and troubled to learn of the massive data breach at Equifax involving 145.5 million American consumers. This breach has the potential to shake consumer confidence in our payments and financial systems for years. In November 2017, ICBA filed suit in the U.S. District Court for the Northern District of Georgia to require Equifax to compensate all community banks harmed by the breach. The complaint cites the myriad damages caused by the breach, such as, for example, the costs of customer credit freezes, protective measures to deter and/or prevent fraud, and cancelation and replacement of payment cards. For a longer-term solution, ICBA also asks the court to require Equifax to improve its security infrastructure to prevent future data breaches.

Create Incentives to Strengthen Data Security

Changes should not be limited to the CRAs but should extend to all entities that hold, store, or process personally identifiable information. Bad actors will continue to look for weaknesses in every link in the chain and future breaches will occur. The goal is to decrease the overall number and severity of data breaches. To strengthen any weak links, ICBA recommends creating a legal structure in which the entity that incurs a breach – be it a retailer, CRA, or other entity – bears financial liability for the cost of the breach.

When a breach occurs at any point in the financial services chain, community banks take a variety of steps to protect the integrity of their customers' accounts, including, among other things, monitoring for indications of suspicious activity, changing customer identity procedures, responding to customer inquiries, reimbursing customers for confirmed fraudulent transactions, modifying customer limits to mitigate fraud losses, and blocking and reissuing payment cards of affected account holders at a cost to the community bank. Deposit account-holding and payment card-issuing banks repeatedly bear these costs up front because prompt action following a breach is essential to protecting the integrity of customer accounts. But these costs should ultimately be borne by the entity that incurs the breach, not by the party protecting the consumer. This is not only a matter of fairness; a liability shift is needed to properly align incentives for entities that store consumer financial and personally identifiable data to strengthen their data security. When breaches have a material impact on entities' bottom line, they will quickly become more effective at avoiding them.

Barring a shift in liability to the breached entity, community banks should continue to be able to access various cost recovery options after a breach.

A National Data Security Breach and Notification Standard is Vital

Many states have enacted laws with differing requirements for providing notice in the event of a data breach. This patchwork of state notification laws does not establish a uniform, baseline standard for the holders of sensitive data. A national notification standard is needed and should be accompanied by GLBA-like data security standards for all participants of the financial system to provide consumers a greater level of protection. This national data security standard should include various cost recovery options, including but not limited to a meaningful private enforcement mechanism. Federal banking agencies should continue to set the notification standard for financial institutions.

It is equally important that community banks receive timely notification concerning the nature and scope of any breach when bank customer information, such as account or payment card numbers, may have been compromised. Expeditious notification is critical to loss mitigation.

Unintended Consequences Must Be Avoided

ICBA is eager to work with this committee on constructive proposals to strengthen data security. In evaluating proposals, we ask this committee to be mindful of unintended consequences that could result for consumers, community banks, and the payments and financial systems. These systems are highly complex, and the consequences of ill-considered policies are hard to predict.

Closing

Thank you again for convening today's hearing. Data breaches are among the highest concerns of America's community bankers. ICBA looks forward to continuing to work with the committee to promote customer security and protect against costly and damaging data breaches.

STATEMENT FOR THE RECORD

ON BEHALF OF

THE NATIONAL ASSOCIATION OF CONVENIENCE STORES

AND

THE SOCIETY OF INDEPENDENT GASOLINE MARKETERS OF AMERICA

FOR THE

HEARING OF THE HOUSE FINANCIAL SERVICES SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

FEBRUARY 14, 2018

"Examining the Current Data Security And Breach Notification Regulatory Regime"

Chairman Luetkemeyer, Ranking Member Lacy Clay and members of the subcommittee, thank you for giving us the opportunity to submit this statement for the record on the topic of the current data security and breach notification regulatory regime. We are submitting this statement on behalf of both the National Association of Convenience Stores (NACS) and the Society of Independent Gasoline Marketers of America (SIGMA).

NACS advances the role of convenience stores as positive economic, social and philanthropic contributors to the communities they serve. The U.S. convenience retail industry, with more than 154,000 locations nationwide selling fuel, food and merchandise, serves 160 million customers daily—half of the U.S. population—and has sales that are 10.8% of total U.S. retail and foodservice sales. NACS has 2,100 retailer and 1,750 supplier members from more than 50 countries.

SIGMA represents a diverse membership of approximately 270 independent chain retailers and marketers of motor fuel. Ninety-two percent of SIGMA's members are involved in gasoline retailing. Member retail outlets come in many forms, including travel plazas, traditional "gas stations," convenience stores with gas pumps, cardlocks, and unattended public fueling locations. Some members sell gasoline over the Internet, many are involved in fleet cards, and a few are leaders in mobile refueling.

Collectively, NACS and SIGMA represent an industry that accounts for about 80 percent of the motor fuel sales in the United States. And, this is truly an industry of small businesses. While many motor fuel outlets have agreements to use the brand names of major oil companies, those oil companies have largely exited the retail market. The vast majority of those branded outlets are locally owned. For example, more than 70 percent of the NACS' total membership is composed of companies that operate ten stores or less, and more than 60 percent of the membership operates a single store.

NACS and SIGMA joined a letter to the Subcommittee along with [groups] laying out four principles that all of the organizations believe should underlie any data breach legislation. With this testimony, we will expand on that letter to explain the interest our members have in data breach legislation, note how the payment card system impacts our data security efforts, provide background on data breaches, note the current state of the law on data breach notification, and walk through in more detail the reasoning behind some of the elements of data breach legislation that we consider to be most important.

I. Convenience and Motor Fuel Outlets Interest in Data Breach Legislation

With so many small businesses, some may wonder why our industry is concerned about data breaches. Our retailers typically do not store much information about their customers. They store employee information, but the primary reason data breaches affect these small, medium, and larger businesses is that these retailers handle payment card information in order to facilitate transactions that occur every day. In light of the number of fuel and other transactions that our industry engages in, we handle approximately one of every thirty dollars spent in the United States. In fact, our retailers serve about 160 million people per day – around half of the U.S. population. And, a majority of those transactions are made using payment cards.

II. The Payment Card System in the United States

Unfortunately, in the United States, payment card information is more vulnerable and enticing to data thieves than it should be. The dominant payment card networks, Visa and MasterCard, control the security of payment cards through promulgating their own proprietary specifications for those cards and their use as well as through the Payment Card Industry (PCI) organization they created and dominate. PCI not only sets data security standards for cards and card issuance, but also for retailers, like NACS and SIGMA members, that accept such cards. This creates an odd dynamic. The companies we represent, and other retailers, do not decide their own data security standards, the payment card networks do that.

Having PCI set data security standards for retailers has not worked well. PCI has consistently put the profits of the companies that control it (principally, Visa and MasterCard) before good security. They have set standards that are both more expensive for retailers than they should be and less effective at providing security than they should be. That is a remarkable combination. Unfortunately, as card security expert Avivah Litan of Gartner Research has written, "The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history."[1]

Standard-setting will only work when every industry is involved and the standards body is not slanted toward any particular sector. Data security is too important for those types of myopic approaches.

One example of a failure of security in this country is the prohibition that Visa in particular has placed in the way of merchants that want to use personal identification numbers (PINs) to protect against fraud. The cheapest, most effective way to better protect against the fraudulent use of payment card numbers is to require another piece of information with those numbers in order to make them useable. The financial industry knows this well. That is why, every time any one of us uses a payment card – whether it's a debit or a credit card – to access our accounts at an automated teller machine (ATM), we enter a PIN. If we don't enter a PIN, we don't get to engage in a transaction. The account number of the card is meant to demonstrate the actual card is there and being used (though this has become less effective in the last generation leading to the move to computer chips in cards throughout the world), and the PIN is meant to demonstrate that the person using the card is the person authorized to do so. *It does not make sense that the same financial institutions that insist a PIN is used to authenticate the person when someone tries to enter into a transaction with them, do not want consumers to have to enter a PIN when they enter into a transaction with a merchant.*

What does this mean for the security of payment card data? Well, if payment card numbers themselves could not be monetized, there would be far less financial incentive for thieves to try to steal that information. PIN numbers are harder to steal than payment card numbers because PINs are typically encrypted as they are entered and remain that way for most of their travels through the payment card system. The major breaches that have garnered news attention in the recent past – at financial institutions and at merchants – have not involved the

[1] "How PCI Failed Target and U.S. Consumers," by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, available at http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/.

loss of PINs. There is some ability for data thieves to guess some PINs and, at the margins, find some ways to monetize payment card data even when PINs are required. But thieves' ability to make money from stolen payment card numbers is greatly diminished when transactions need a PIN.

Allowing merchants to use the protection of PINs is not a silver bullet solution. There is far more to it than that. But, the failure of the financial industry to make that simple move, and one that is cheap and easy for the vast majority of merchants, is emblematic of the problems we all face protecting payment card data from breaches today.

III. The Picture of Data Breaches

Data thieves steal information from every type of organization in the United States. No one is immune. Manufacturers, utilities, services companies, health care providers, educational institutions, not-for-profits, telecommunications companies, banks, credit unions, payment card networks, payment card processors and merchants have all suffered data breaches. In fact, government agencies also suffer data breaches. Victims of breaches have even included the Defense Department and National Security Agency. These organizations are true experts in this area and go to great lengths to protect their systems. But, again, no one is immune.

Unfortunately, data thieves today include foreign countries and well-funded, sophisticated organized crime organizations, among many others. These thieves know where vulnerabilities are and relentlessly work to exploit them. It is very difficult to protect against these thefts. U.S. entities that suffer data breaches are victims of these crimes. That does not mean they shouldn't have any responsibilities when they are victimized, but it's worth remembering when some want to take a punitive approach to those who suffer breaches.

The Verizon Data Breach Investigations Report is the most comprehensive summary of data threats. The 2017 report (examining 2016 data) determined that there were 42,068 data security incidents reported by industry, educational institutions and governmental entities and that 1,935 of those had confirmed data losses. Of those with confirmed data losses, the financial industry suffered 24%, healthcare companies had 15%, public institutions (including governmental entities) had 12%, the information technology and telecommunications sector had just less than 6%,[2] and the retail industry had less than 5% of the incidents with confirmed data losses. As noted above, other sectors suffered breaches as well. When reviewing these numbers, it is worth keeping in mind that there are approximately 1,000 times as many retailers in the country as there are financial institutions.

IV. Current State of the Law

Before getting into questions about a potential federal data breach law, it is worth taking a look at the current state of the law. A total of 52 U.S. states and territories have data breach laws on the books today. Companies comply with these laws every day. This is not an area in which there is a lack of regulation.

[2] The information industry was described in the report as "the heavy hitters from a record-loss standpoint." 2017 Verizon Data Breach Investigations Report at 7.

Many of these 52 laws are very similar. While there may be some benefits to streamlining this system by having one federal law that pre-empts these 52 different laws, that should only be done if it can improve upon the current law. It would be simpler and cheaper for businesses to comply with one law than with many, but that is not the only value at stake in this discussion. Any effort to write federal legislation should take care not to introduce problems that the current law does not have.

V. Elements of Data Breach Law

There are several elements that we see as important to a federal law on data breach and we outlined four key principles for such legislation in the letter we sent along with other, like-minded associations. Those four key principles are: establishing a uniform nationwide law; setting reasonable data security standards; maintaining an appropriate FTC enforcement regime; and ensuring all breached entities have notice obligations. Below, we further explore and explain these principles. First, we explain that the law should not have holes in it that result in consumers not getting notice. Second, we emphasize that the law should create a level playing field for businesses so that it does not introduce gaps that data thieves can exploit and does not overly burden any particular sector of the economy. Third, we set forth our view that the law needs to have sufficient flexibility to cover the many different circumstances arising from different data breaches. This includes requiring notice only when it makes sense to do so and allowing sufficient flexibility on timing for proper investigations of data incidents to take place. Fourth, we explain why the law should not take a punitive approach to businesses that have their data stolen by thieves. Fifth, we discuss why, if there is going to be a federal law in this area, it should pre-empt state laws. There is no need for a fifty-third data breach law.

a. Don't Create Notice Holes

In most instances, when data breaches happen today, consumers can have confidence that if the breach exposes data in a way that may harm them, they will get notice. The 52 different laws around the country help ensure that this happens. That is as it should be.

There are, however, exceptions to this general confidence. The data breach guidance put in place pursuant to the Gramm Leach Bliley Act (GLBA), for example, does not provide such confidence when financial institutions have data breaches. GLBA guidance says that banks and credit unions should have response plans in place in case their systems are breached, but those response plans are not actually required.[3] GLBA guidance recommends that financial institutions have plans in place to provide consumer notification of data breaches, but again those plans are not required.[4] Following a breach, GLBA guidance says that banks should conduct an

[3] 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) [hereinafter *Guidelines*] at ¶ III, C.

[4] Incident Response Guidance, 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) [hereinafter *Response Guidance*].

investigation to determine the likelihood that information has been or will be misused as a result of the breach, but that investigation is not required.[5] GLBA guidance also provides that if a financial institution determines that customer information has been or is likely to be misused then the institution should notify its customers.[6] But, here again, such notice is not required. In short, GLBA results in a system of law in which financial institutions have discretion over how closely to look at their data breaches and whether to inform their customers, if at all. In fact, we are not aware of any financial institutions that have been investigated and fined for not adequately looking into a data breach or not providing customers with notice of such a breach.

Thankfully, the majority of state laws help patch this major shortcoming in federal law. Based on our analysis, more than two-thirds of the fifty-two state and territorial data breach laws cover banks while less than one-third of them exempt banks. That helps, but it isn't good enough to provide consumers with the confidence they should have that they will get notice when it is warranted. Any federal law on data breach needs to fix this hole in the current notice system or it is ignoring the most prominent shortcoming of the current system of notice for data breaches around the country.

b. Create a Level Playing Field

Ensuring there are no holes in data breach notice provisions goes hand-in-hand with establishing a level playing field for businesses that handle data. Many types of data are transmitted between different businesses on a regular basis but this is particularly true of payment card data. In fact, merchants, data line providers, processors, acquiring banks, card networks, and card issuers transmit data back-and-forth among one another hundreds of millions of times per day. If data breach legislation focuses on some of these businesses and does not cover others the same way, a couple of problems will result. One is that the lack of standards for some will, because the businesses will operate with different incentives, lead to data security gaps that thieves will exploit. Two is that some businesses will take on the brunt of the costs and reputational harms that can come with notice responsibilities even when they are not responsible for some of those breaches. That would not be appropriate.

The problem of data security weaknesses in the transfer of data among businesses is already part of the landscape. For example, merchants are required by the payment card companies to encrypt payment card data when they hold it on their systems. But, financial institutions are not required to be capable of accepting that data in encrypted form. The result is that data must be de-encrypted as it runs through the payment system in order to complete a transaction.[7] Data thieves have targeted these points of vulnerability in past data breaches. If we are going to have federal legislation, it should avoid creating similar gaps by covering everyone in the payment data chain with the same laws.

For some reason, telecommunications providers have argued that they should not have the same responsibilities as other companies that handle data. Some have raised a fallacious concept to justify this position. They claim that data lines controlled by telecommunications

[5] *Id.*
[6] *Id.*
[7] The Nilson Report, Issue 934, Sept. 2009 at 7.

providers are "dumb pipes." Nothing could be further from the truth. Data lines include switches and routers that can monitor the carriage of data, watch for problems, and ensure transmissions get to the right place. This is all necessary to making the system operate correctly.

These complexities are why the Federal Communications Commission and the Congress have even considered the issue of net neutrality. If telecommunications lines were actually "dumb" they could not be anything other than neutral. We are not aware, for example, of anyone calling on this committee to examine water or sewer line neutrality. The phrase and concept of "dumb pipes" simply has no place in the discussion of data breaches.

The switches and routers in telecommunications lines consist of millions of lines of computer code – and they have vulnerabilities. In fact, by law these systems are required to have backdoors allowing the companies to tap those lines and access the data being sent. Those requirements are in place so that law enforcement can gather information being transmitted when appropriate. When legitimate actors can access communications in transit to monitor data, unfortunately, illegitimate ones can as well. No one's system is completely immune from data thieves. Telecommunications providers, just like other businesses, have suffered data breaches in the past. There is no principled basis for absolving these companies from the responsibilities that others have when their systems are breached.

That would be true even if the telecommunications system were "dumb." Petroleum pipelines, for example, do not have the level of sophisticated software controlling the flow of contents through them that telecommunications lines do. Even though one might refer to them as "dumb" pipes, if petroleum pipelines are breached then the responsibility for the consequences are clear – the pipeline must deal with that. Pipelines do not tell the shippers of product that the shippers must clean up the spill. Yet, that is the odd construct that telecommunications carriers are urging with respect to their data breaches.

The bottom line is that the business that is breached should shoulder the burdens of notice of that breach. Other businesses, for example, should not carry the burden, reputational or otherwise, when telecommunications companies suffer breaches. That is especially true of small businesses. These businesses work hard to secure their own systems, but they don't have the same resources or sophistication to follow the work of data thieves that big businesses (including many telecommunications companies) do. If a telecommunications provider or financial institution tells a small business that the small business suffered a breach, that small business usually accepts that as fact. But the initial assessment of where a breach occurred is often wrong and if the telecommunications provider and financial institution do not have their own legal responsibilities regarding breaches of their systems, many breaches will be laid at the doorstep of others and no one will ask more questions. If a federal law is going to empower regulators to look into these situations, they must have the latitude to look at everyone involved to ensure they live up to their responsibilities – and don't simply pawn off those responsibilities onto smaller players with fewer resources.

c. Provide Flexibility

Data breaches can be difficult to detect and it can be even more difficult to determine the full extent of some of them. The complexity of breaches has consistently increased over time along with the increased sophistication and funding of organized crime. Providing public notice of data breaches before the full extent of a breach is known, and therefore before a business can be sure that its system is fully secure, can create increased risk for consumers and business. If data thieves become aware that they have been detected, which notice would make clear, they often try to quickly grab as much additional data as they can as fast as they can. That is not a risk that legislation needs to create by setting an arbitrary timing requirement for notice. While many laws provide exceptions to notice requirements when law enforcement requests a delay, that alone may not be sufficient to protect against this type of problem.

In order to avoid setting a requirement that notice be given before a system is fully secured, a flexible timing requirement that includes the concept of the business need for fully protecting against further data theft would be wise.

d. Avoid Punitive Approaches

As noted previously, companies that suffer data breaches are victims of crimes. Without question, consumers and businesses that have their data stolen are victims of crime as well. Some media accounts of these incidents, however, seem to overlook what a significant and difficult problem it is to protect against data thieves. If the Defense Department and NSA can be hacked, it demonstrates how difficult the challenge is for private businesses to fully protect themselves. Given the difficulty, overly punitive measures are not appropriate in these situations. We are not saying that a failure to follow a notice law should not have any penalty associated with it. That can be necessary in some cases to get some businesses to comply. But the penalties should not be ones that are overwhelming, especially for small businesses. The goal should be to help businesses comply with the law to the greatest extent possible – not to play a "gotcha" game that leads to large fines. The costs of dealing with breaches, including paying forensic experts, lawyers, fraud costs, and dealing with reputational harms, already create strong economic incentives for businesses to try to avoid breaches. If one occurs, it should not simply be an excuse to pile on additional financial hits.

In fact, for most businesses, the risk of reputational harm is better motivator than any fines that legislation could put in place. That reputational harm can dramatically cut into a business' revenues and threaten its existence. The surest way to put reputational risks front and center to motivate good data security practices is to ensure that any breached business must be responsible for fulsome notice to consumers of its breaches. That public disclosure ensures that the business' reputation will have to answer for the incident. But, allowing any industry the ability to keep breaches secret or hand-off its notice responsibilities to others will reduce the deterrent effect of notice and reduce the motivation for strong data security practices.

e. Pre-empt State Laws

As noted, there are two primary rationales for having a federal data breach law in light of the fact that the 52 state and territorial laws that currently exist cover the area well already. The first reason is to plug the holes that exist in the coverage of these laws today. Most prominently, a federal law would improve on the current set of data breach laws by removing the overly broad discretion given to financial institutions in the states that exempt them from their laws. The second reason for a federal law is to create a simpler and more efficient notice system. That way, businesses would only have to comply with one federal law rather than as many as 52 different ones. That efficiency can only be achieved if the state laws in this area are pre-empted. To the extent that pre-emption is not clear, a federal law would become the fifty-third law to comply with and the second rationale for having a federal law at all would be undermined. This pre-emption is necessary then for a federal law to make sense.

Pre-emption, however, makes it even more important to get any federal data breach law right. The state system currently ensures that people get notice in most of the situations that they should. That should not be undermined in the process of creating a federal law. In our view, the principles we've laid out above, if followed, would help protect against the potential negative consequences that could come from pre-emption. Given the hazards, however, we urge that the committee take its time and not rush through legislation before fully weighing all of the trade-offs between a federal bill and the state and territorial laws on the books.

* * *

We appreciate the subcommittee providing us with this opportunity to submit our views on federal data breach legislation. We look forward to working with you as the committee continues to consider this topic.

NAIC National Association of Insurance Commissioners & The Center for Insurance Policy and Research

Statement for the Record
From the National Association of Insurance Commissioners
for the U.S. House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
Hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime"
February 14, 2018

Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, the National Association of Insurance Commissioners (NAIC)[1] appreciates the opportunity to submit this written statement for the hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime." State insurance regulators are keenly aware of the potentially devastating effects cyber-attacks can have on consumers and businesses and share your commitment to addressing cybersecurity risks and protecting consumer data. We recognize the importance of cybersecurity risk management and continue to upgrade safeguards to protect the security, confidentiality, and integrity of insurance consumers' information through standards, the examination processes, and model laws.

State insurance regulators have taken a number of steps to ensure the insurers, agents, and brokers we regulate are adequately protecting the many kinds of highly sensitive consumer financial and health information they retain. All states have standards that comply with those set forth in the Gramm-Leach-Bliley Act. Further, in recognition that the standards governing the protection of insurance consumer information must evolve to keep pace with cybersecurity risks, the NAIC adopted the Insurance Data Security Model Law (attached) in October 2017. This model law updates state insurance regulatory requirements relating to data security, the investigation of a cyber event, and the notification to state insurance commissioners of cybersecurity events at regulated entities. The development of this model law involved almost two years of deliberations by insurance regulators that considered and incorporated extensive input from the insurance industry and consumer representatives.

Specifically, the model requires insurers, agents, and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program based on its risk assessment. It also includes requirements for oversight of third-party service providers. The model requires licensees to notify relevant state insurance commissioners of cybersecurity events, including providing a description of how the information was exposed, lost, stolen, or breached; how the event was discovered; the period during which the information system was compromised; the total number of consumers affected in the state; and the efforts being undertaken to remediate the situation. It also grants insurance commissioners the authority to examine and investigate licensees to determine compliance with the law and to remedy data security deficiencies they find during an examination. In an October

[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, NW, Suite 700 • Washington, DC 20001-1509 p [illegible] f [illegible]
CENTRAL OFFICE • 1100 Walnut Street, Suite 1500 • Kansas City, MO 64106-2197 p [illegible] f [illegible]
CAPITAL MARKETS & INVESTMENT ANALYSIS OFFICE • One New York Plaza, Suite 4210 • New York, NY 10004 p [illegible] f [illegible]

2017 report on the asset management and insurance industries, the U.S. Treasury Department endorsed the model and urged its prompt adoption.[2]

Further, we have updated and strengthened existing guidance for examiners regarding information technology systems and protocols to draw more focus to the consideration of cybersecurity during an exam. Specifically, the NAIC Financial Condition Examiners Handbook, which is used by insurance regulators as they examine insurers, incorporates the National Institute of Standards and Technology (NIST) concepts of Identify, Protect, Detect, Respond and Recover. This includes improvements to encourage greater review and testing of cybersecurity exposure, as well as corresponding company controls, during the course of a financial examination. It also includes reviews of insurer cybersecurity training and education programs and incident response plans; post remediation analysis; consideration of third-party vendors; and how cybersecurity efforts are communicated to the board of directors. The NAIC is also updating our Market Regulation Handbook to strengthen sections regarding cybersecurity. We also developed the Cybersecurity and Identity Theft Coverage Supplement for insurer financial statements to gather financial performance information about insurers writing cybersecurity coverage.

In addition to our work improving cybersecurity practices in the insurance sector, we work collaboratively with other state and federal regulators through the Treasury Department's Financial and Banking Information Infrastructure Committee (FBIIC) to facilitate coordination and communication on regulatory approaches to managing and evaluating cybersecurity risk in the financial sector. State insurance regulators are also members of the Cybersecurity Forum for Independent and Executive Branch Regulators, where we discuss best practices and common regulatory approaches to cybersecurity challenges across different sectors of the U.S. economy.

While the NAIC recognizes that cybersecurity and associated regulatory concerns stretch beyond the insurance sector, Congress should not disregard the existing state insurance regulatory framework or inhibit ongoing efforts in the states to adopt cyber laws and regulations in the best interests of insurance consumers. We appreciate your consideration of our views and thank you for the opportunity to submit this written statement for the record. We look forward to continued engagement with you as we work together to improve the cyber resiliency of our nation's financial infrastructure.

---

[2] https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Title

This Act shall be known and may be cited as the "Insurance Data Security Law."

Section 2. Purpose and Intent

A. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.

B. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Drafting Note: The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, *Cybersecurity Requirements for Financial Services Companies*, effective March 1, 2017, such Licensee is also in compliance with this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. "Authorized Individual" means an individual known to and screened by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its Information Systems.

B. "Commissioner" means the chief insurance regulatory official of the state.

C. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this State and whose Nonpublic Information is in a Licensee's possession, custody, or control.

D. "Cybersecurity Event" means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System.

The term "Cybersecurity Event" does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

E. "Department" means the [insert name of insurance regulatory body].

F. "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

G. "Information Security Program" means the administrative, technical, and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information.

H. "Information System" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

I. "Licensee" means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

J. "Multi-Factor Authentication" means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

K. "Nonpublic Information" means information that is not Publicly Available Information and is:

(1) Business related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Licensee;

(2) Any information concerning a Consumer which because of name, number, personal mark, or other identifier can be used to identify such Consumer, in combination with any one or more of the following data elements:

(a) Social Security number,

(b) Driver's license number or non-driver identification card number,

(c) Account number, credit or debit card number,

(d) Any security code, access code or password that would permit access to a Consumer's financial account, or

(e) Biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a Consumer and that relates to

(a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer's family,

(b) The provision of health care to any Consumer, or

(c) Payment for the provision of health care to any Consumer.

L. "Person" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

M. "Publicly Available Information" means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

For the purposes of this definition, a Licensee has a reasonable basis to believe that information is lawfully made available to the general public if the Licensee has taken steps to determine:

(1) That the information is of the type that is available to the general public; and

(2) Whether a Consumer can direct that the information not be made available to the general public and, if so, that such Consumer has not done so.

N. "Risk Assessment" means the Risk Assessment that each Licensee is required to conduct under Section 4C of this Act.

O. "State" means [adopting state].

P. "Third-Party Service Provider" means a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain

a comprehensive written Information Security Program based on the Licensee's Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.

B. Objectives of Information Security Program

A Licensee's Information Security Program shall be designed to:

(1) Protect the security and confidentiality of Nonpublic Information and the security of the Information System;

(2) Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System;

(3) Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and

(4) Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.

C. Risk Assessment

The Licensee shall:

(1) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the Information Security Program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;

(4) Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:

(a) Employee training and management;

(b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Risk Management

Based on its Risk Assessment, the Licensee shall:

(1) Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control.

(2) Determine which security measures listed below are appropriate and implement such security measures.

(a) Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;

(b) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

(c) Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;

(d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;

(e) Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;

(f) Modify the Information System in accordance with the Licensee's Information Security Program;

(g) Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;

(h) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;

(i) Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;

(j) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

(3) Include cybersecurity risks in the Licensee's enterprise risk management process.

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.

E. Oversight by Board of Directors

If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) Require the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security Program;

(2) Require the Licensee's executive management or its delegates to report in writing at least annually, the following information:

(a) The overall status of the Information Security Program and the Licensee's compliance with this Act; and

(b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.

(3) If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.

F. Oversight of Third-Party Service Provider Arrangements

(1) A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and

(2) A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and

secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.

G. Program Adjustments

The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.

H. Incident Response Plan

(1) As part of its Information Security Program, each Licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity, or availability of Nonpublic Information in its possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations.

(2) Such incident response plan shall address the following areas:

(a) The internal process for responding to a Cybersecurity Event;

(b) The goals of the incident response plan;

(c) The definition of clear roles, responsibilities and levels of decision-making authority;

(d) External and internal communications and information sharing;

(e) Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(f) Documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(g) The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

I. Annual Certification to Commissioner of Domiciliary State

Annually, each insurer domiciled in this State shall submit to the Commissioner, a written statement by February 15, certifying that the insurer is in compliance with the requirements set forth in Section 4 of this Act. Each insurer shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commissioner.

Section 5. Investigation of a Cybersecurity Event

A. If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.

B. During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:

(1) Determine whether a Cybersecurity Event has occurred;

(2) Assess the nature and scope of the Cybersecurity Event;

(3) Identify any Nonpublic Information that may have been involved in the Cybersecurity Event; and

(4) Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.

C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will complete the steps listed in Section 5B above or confirm and document that the Third-Party Service Provider has completed those steps.

D. The Licensee shall maintain records concerning all Cybersecurity Events for a period of at least five years from the date of the Cybersecurity Event and shall produce those records upon demand of the Commissioner.

Section 6. Notification of a Cybersecurity Event

A. Notification to the Commissioner

Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met:

(1) This State is the Licensee's state of domicile, in the case of an insurer, or this State is the Licensee's home state, in the case of a producer, as those terms are defined in [insert reference to Producer Licensing Model Act]; or

(2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this State and that is either of the following:

(a) A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

(b) A Cybersecurity Event that has a reasonable likelihood of materially harming:

(i) Any Consumer residing in this State; or

(ii) Any material part of the normal operation(s) of the Licensee.

B. The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.

(1) Date of the Cybersecurity Event;

(2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any;

(3) How the Cybersecurity Event was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the Cybersecurity Event;

(6) Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;

(8) The period during which the Information System was compromised by the Cybersecurity Event;

(9) The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;

(10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(11) Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur;

(12) A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event; and

(13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.

C. Notification to Consumers. Licensee shall comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when a Licensee is required to notify the Commissioner under Section 6A.

D. Notice Regarding Cybersecurity Events of Third-Party Service Providers

(1) In the case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, of which the Licensee has become aware, the Licensee shall treat such event as it would under Section 6A.

(2) The computation of Licensee's deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.

(3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third-Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.

E. Notice Regarding Cybersecurity Events of Reinsurers to Insurers

(1) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

(2) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification

law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

F. Notice Regarding Cybersecurity Events of Insurers to Producers of Record

In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected Consumers as soon as practicable as directed by the Commissioner.

The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.

Section 7. Power of Commissioner

A. The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].

B. Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this State which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.

Section 8. Confidentiality

A. Any documents, materials or other information in the control or possession of the Department that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section 4I, Section 6B(2), (3), (4), (5), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.

B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A.

C. In order to assist in the performance of the Commissioner's duties under this Act, the Commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies,

with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;

(3) May share documents, materials or other information subject to Section 8A, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; and

(4) May enter into agreements governing sharing and use of information consistent with this subsection.

D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in Section 8C.

E. Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 9. Exceptions

A. The following exceptions shall apply to this Act:

(1) A Licensee with fewer than ten employees, including any independent contractors, is exempt from Section 4 of this Act;

(2) A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee is compliant with, and submits a written statement certifying its compliance with, the same;

(3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 and need not develop its own Information Security Program to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.

B. In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.

Section 10. Penalties

In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].

Section 11. Rules and Regulations [OPTIONAL]

The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act.

Drafting Note: This provision is applicable only to states requiring this language.

Section 12. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 13. Effective Date

This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC).

2017 4th Quarter (adopted by Executive/Plenary via conference call)

February 12, 2018

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions & Consumer Credit
House Financial Services Committee
2230 Rayburn House Office Building
Washington, DC 20515-2503

The Honorable Lacy Clay
Ranking Member
Subcommittee on Financial Institutions & Consumer Credit
House Financial Services Committee
2428 Rayburn House Office Building
Washington, DC 20515-2503

The National Multifamily Housing Council (NMHC) and National Apartment Association (NAA) applaud the Subcommittee for calling a hearing entitled "Examining the Current Data Security and Breach Notification Regulatory Regime." We appreciate the Subcommittee exploring the current regulatory landscape surrounding data security and breach notification standards and the impact it has on both businesses and consumers.

For more than 20 years, NMHC and NAA have partnered on behalf of America's apartment industry. Drawing on the knowledge and policy expertise of staff in Washington, D.C., as well as the advocacy power of more than 160 NAA state and local affiliated associations, NAA and NMHC provide a single voice for developers, owners and operators of multifamily rental housing. One-third of all Americans rent their housing, and 39 million of them live in an apartment home.

Rental housing owners and operators, and their third-party service providers, rely heavily on highly sensitive, personal data about apartment applicants, residents and employees to run their day-to-day business. Given the value of this information to thieves and the ever-expanding cyber-threat landscape, rental housing owners and operators have made defense against cyber vulnerabilities and protecting industry data a top priority. We are pleased that the Subcommittee has placed cybersecurity and consumer privacy high on its agenda, and we join policymakers in calling for enhanced data and consumer protections.

As the Subcommittee considers solutions to bolster consumer and data protection, NMHC/NAA believe that any federal legislation should provide for:

- A clear Federal preemption of the existing patchwork of often conflicting and contradictory state data security, privacy and breach notification laws.

- A reasonable, flexible and scalable national standard for data protection. Specifically, when establishing compliance obligations, this standard must consider the needs and available resources of small businesses as well as large firms and the sensitivity of the data in question.
- A clear assignment of financial and legal liability to the entity that actually suffered the breach, particularly in the case of third-party breaches.
- A requirement that third-party service providers must notify their customers of any breach and allow them to notify the consumer of the breach if they so choose.

We thank you for the opportunity to present the views of the rental housing industry as you continue deliberations to enhance data security and breach notification standards. NMHC/NAA stand ready to work with Congress to create a federal data and breach notification standard that recognizes the unique nature and needs of the rental housing industry while ensuring the data that our members collect, use and maintain is secure.

Sincerely,

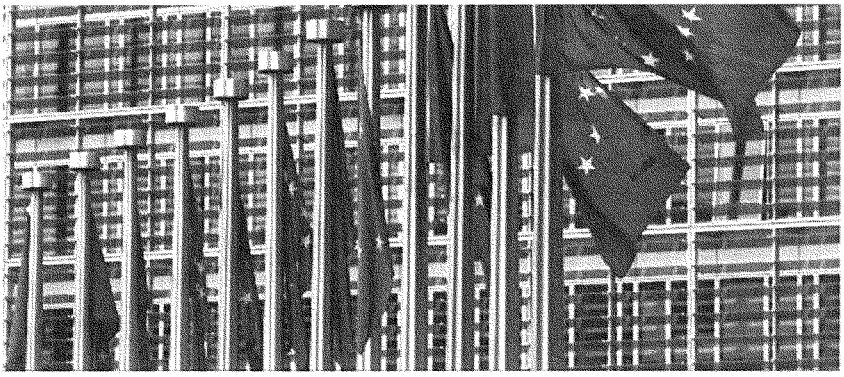
Cindy Vosper Chetti
Senior Vice President, Government Affairs
National Multifamily Housing Council

Greg S. Brown
Senior Vice President, Government Affairs
National Apartment Association

cc: Members of the Subcommittee on Financial Institutions & Consumer Credit

Europe's New Data Protections Expected to Spill Over into U.S.

The European Union is enacting sweeping new data protections while Congress dithers, and the impact on Americans' data security could be significant.



AP Photo/Yves Logghe

Brendan Bordelon
@BRENDANBORDELON

SHARE
TWEET
EMAIL
ADD TO BRIEFCASE

Feb. 12, 2018, 6:53 p.m.

When credit-reporting agency Equifax first revealed the theft of personal and financial data from more than 145 million of its customers last fall, some cybersecurity experts believed the time was finally ripe for Congress to craft data-security and breach-notification rules for all aspects of the U.S. economy.

Months later, most now admit their expectation of congressional action was misplaced. While the steady drumbeat of data breaches continues and lawmakers still give lip service to the notion of federal standards beyond the health care and financial sectors, the broader political gridlock gripping Washington seems to have stymied Capitol Hill.

MOST READ
1 Can Corker Survive a Republican Primary?
2 New Initiatives Push for Diverse Hiring on the Hill
3 Bob Corker's Political Self-Destruction
4 Trump's Publication Food-Stamp Plan
5 The Congressional Turnover List

WHAT WE'RE FOLLOWING SEE MORE »
GEORGE BANKS SERVES ON NEC
Another White House Official Quits Amid Security Clearance Hurdles
40 MINUTES AGO

See more stories about—

Business And Regulation

Foreign Policy

Technology

Cuba

Senate

House Of Representatives

Congress

"I don't suspect that there'll be [federal legislation] right now," said Jocelyn Aqua, a privacy and cybersecurity expert at consulting firm PwC. "I would've thought with Equifax, that would've been the closest."

But the absence of wide-ranging federal rules governing corporate cybersecurity doesn't mean Americans are stuck in limbo when it comes to data privacy. In fact, most experts believe that over the next several years, consumers will experience a significant increase in the level of protection and notification they receive when their corporate-held data is stolen or comes under threat.

The catalyst of this expected shift is a set of sweeping new data-privacy rules that regulators in the European Union will start enforcing in May. Dubbed the General Data Protection Regulation, these rules dramatically expand the types of consumer data protected under EU law, increase the ability of European consumers to exert control over their data, and give companies a slim 72-hour window to disclose breaches to consumers and regulators.

Any American company that does business with Europeans—even those with no physical presence on EU soil—will have to comply. And regulators are expected to dish out up to $6.4 billion in fines per year to recalcitrant companies, making it imperative for U.S. firms to change their privacy practices accordingly.

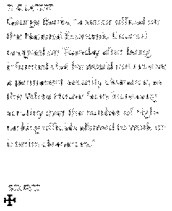
"The threat of 2 to 4 percent of global revenue in fines for violations is real, especially since the EU has demonstrated it has no qualms throwing large fines at U.S. tech companies," said David O'Brien, a senior researcher at Harvard University's Berkman Klein Center for Internet & Society.

Though the new law applies only to European consumers, it's expected to also have a powerful impact on the protections afforded to Americans.

Because it's difficult and expensive for companies to navigate a patchwork of varying data-protection standards, many U.S. firms will likely harmonize their global data-privacy and breach-notification practices with Europe's strict new model.

"We're looking at this completely holistically for the protection and privacy of our customers," said Grant Bourzikas, the chief information security officer at cybersecurity firm McAfee.

Bourzikas made clear that the majority of protections granted to European consumers will be passed on to McAfee's customers in the U.S. "We're embedding it in how we operate as an organization," he said.



Tom Pendergast, the chief security and privacy strategist at consulting firm MediaPro, believes major U.S. firms such as Microsoft, Boeing, General Motors, and Chevron will follow suit. "No company wants to manage multiple data-protection practices," he said. "So they tend to skew toward the highest standard."

That standard may also extend to companies that don't have any European customers but supply larger firms that do. "These big global companies are pushing those requirements down through their supply chain," said Pendergast, who expects the GDPR to initiate "a ripple effect throughout the U.S. economy."

For many Americans, one of the most infuriating aspects of data-privacy standards is the lag time between when companies discover a breach and when they report it to their customers—a gap that can sometimes extend for months or even years.

But because the GDPR gives companies just three days to sound the alarm once a breach of European data is discovered, that lag time could be significantly reduced for Americans affected by the same breach.

"You'll have a significant population of individuals receiving notification for types of personal-data compromises," said Kimberly Peretti, a cochair of the cybersecurity wing of the law firm Alston & Bird. "That may trigger individuals in other locations—when they hear about the press related to it, or employees talk about it—that could certainly create the question to the company, 'Am I impacted?'"

And many firms will be hard-pressed to explain to American consumers why the new protections and notification requirements for Europeans aren't necessary on their side of the pond. "There will have to be some consideration of how that looks," Aqua said.

Until recently, one of the largest hurdles to greater consumer control over their corporate-held data was a technical one. Before the advent of the GDPR, few companies had the tools and processes in place to go into consumer databases and alter, extract, or delete data.

Now that the EU has required companies to build and develop those tools, many firms are expected to deploy them to the United States as well as Europe. "This kind of forces a revolution in data-handling practices," said Pendergast.

Still, there will inevitably be differences in how European and American data is handled by companies. Some experts believe the new 72-hour breach-notification window is far too narrow, and that Americans will receive less information and have to wait longer after a data breach than people across the pond. It's also not clear whether companies with

business models built on amassing mounds of consumer data will be comfortable giving Americans the ability to remove or significantly alter that data.

"We generally don't follow the EU's footsteps in privacy law and policy," said O'Brien. "Although we share certain values and principles in practice, the U.S. has historically taken a very hands-off approach to commercial privacy."

But as data breaches continue to make headlines, other experts believe the blasé corporate culture surrounding data privacy in the U.S. is changing rapidly.

"For big American companies, it's not just being in compliance that matters," said Pendergast. "Being trustworthy is really critical."

Opening Statement
The Honorable Maxine Waters, Ranking Member, Financial Services Committee
Hearing entitled, "Examining the Current Data Security and Breach Notification Regulatory Regime"
Wednesday, February 14, 2018, 10:00 a.m.

Thank you Chairman Luetkemeyer for convening today's hearing and to each of the witnesses for being here today.

The massive breach at Equifax exposed the sensitive personal information of over 145 million Americans, leaving them vulnerable

to identity theft, fraud and other forms of harm.

Yet, rather than clean up the mess it had created through its failure to implement adequate security protocols, Equifax botched the response to the breach, exacerbating the risk of harm that so many Americans now face.

Not only did Equifax fail to take action to fix the software vulnerability once the Department of Homeland Security brought it to the company's attention, but Equifax waited for weeks before notifying law enforcement and affected consumers. If that wasn't bad enough, Equifax launched and directed consumers to a defective website where consumers were told they could find out whether their information had been

compromised. The website's authentication protocol, however, required consumers to provide the same social security numbers that had just been exposed. The site was later hacked, infected with malware, and at one point the company even directed consumers to another fake website thinking it was their own.

Unfortunately, these failures are just the tip of the iceberg in an industry that is fundamentally broken.

As, the Democratic Witness Mark Rotenberg recently put it recently, quote, "the essential problem with the credit reporting industry is that it does not work," unquote.

I couldn't agree more, and that is why, I have long called for a complete overhaul of the entire credit reporting system. It's also why I recently re-introduced H.R. 3755, the "Comprehensive Consumer Credit Reporting Reform Act" that would do just that.

In addition to common sense measures that strengthen consumer's ability to protect their

credit, my bill shifts the burden of removing mistakes from credit reports onto the credit bureaus and furnishers, and away from consumers; limits credit checks for employment purposes; and reduces the time period that negative items stay on credit reports, among many other key reforms.

These reforms, and ongoing efforts at the state level, should be included in any

product this Committee develops to safeguard consumer's data.

I look forward to the witnesses' testimony and I yield back the balance of my time.

QUESTIONS FOR THE RECORD
REP. DENNY HECK (WA-10)

Financial Institutions Subcommittee Hearing:
"Examining the Current Data Security and Breach Notification Regulatory Regime"

Hearing Date: February 14, 2018

Questions for All Witnesses:

1. **I have been trying to look into information on how many of the 145 million victims of the Equifax hack have had fake accounts opened in their name in the last several months, and there doesn't seem to be any public info on that.**

    a. **Does that exist? It seems like a spike of identity theft cases would be something we'd want to know quickly about so that people could freeze their credit or take other steps to protect themselves.**

    b. **Is this something that is publicly reported? Should it be?**

BSA Response:

I am unaware of any public resource that provides real-time reporting regarding the incidence of identity theft. The most comprehensive database of such information I am aware of is the Consumer Sentinel Network, an investigative tool and complaint database for law enforcement personnel that is administered by the Federal Trade Commission. The Consumer Sentinel Network catalogs all consumer complaints related to financial issues, including identity thefts, filed with the FTC, FBI, US Postal Inspection Service, Better Business Bureau, the Identity Theft Assistance Center, the Internet Crime Complaint Center, and the National Fraud Information Center. Access to the database is restricted to registered law enforcement personnel, and is used as a tool to spot trends, identify questionable business practices, and enforce the law. However, the FTC does issue an annual public report that documents the number of incidents received by the Consumer Sentinel Network. According to the 2017 report, US consumers experienced 371,061 instances of identity theft in 2017, accounting for approximately 13.87% of the 2.68 million consumer complaints documented in the Sentinel database. [1]

2. **One thing I heard in the aftermath of the Equifax breach was that it wasn't really that harmful on the margin because all of the information that was stolen in the breach was already available on the "dark web" anyway. Do you agree? I'm skeptical of these claims, but I'd like to hear your opinions.**

BSA Response:

I share your skepticism. Data breaches have a corrosive effect on consumer trust in the digital economy irrespective of whether the impacted data might have also been exposed through earlier security incidents. Although it may be difficult to correlate financial crimes to specific data breaches, we do know that the cumulative impact of these incidents is shaking consumer confidence in the digital economy. [Indeed, a 2017 Pew Research Center study found that nearly two-thirds of Americans (64%) have personally been affected by a major data breach, and nearly

---

[1] Federal Trade Commission, *Consumer Sentinel Network: Data Book 2017* (March 2018), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf

half of all Americans (49%) now feel that their personal information has become less secure in recent years.[2] This erosion of consumer trust is a worrying trend and potential threat to a key pillar of the United States' international competitive advantage.] As noted during my testimony, US economic growth and job creation have been driven in recent years by data-enabled efficiencies. In every industry, the analysis of data has made businesses more agile, responsive, and competitive, boosting the underlying productivity of many key pillars of our economy. The public's embrace of the digital economy cannot be taken for granted. Ensuring that customers have confidence in the security and privacy of their personal data is vital to ensuring their trust in digital services.

3. **There are government agencies like the National Transportation Safety Board and Chemical Safety Board that are purely responsible for investigating and reporting on how disasters happen and what we can do to avoid them in the future.**

   I'm wondering about a Computer Network Safety Board that would investigate breaches like Equifax and issues reports on why the systems failed and how they could be made better. Is that an idea you think is worth exploring?

BSA Response:

A range of federal agencies play roles in disseminating actionable information to help relevant stakeholders protect themselves from cyberattacks. For instance, the Federal Trade Commission plays a critical role in investigating data breaches resulting in consumer harm. In addition to making available relevant information derived from their investigations, the FTC maintains the "Start with Security" guide for businesses that draws security lessons from past enforcement actions. Outside of the regulatory enforcement context, the Department of Homeland Security is the lead agency responsible for responding to "significant" cyber incidents. In this capacity, the National Cybersecurity and Communications Center assists network owners in mitigating potential vulnerabilities by sharing information across the public and private sectors.

In considering your question, it is important to keep in mind that virtually all companies that suffer a data breach are themselves the victims of a crime. It is therefore critical that law enforcement have the tools and resources needed to investigate the crime and prosecute offenders.

4. **When I meet with grocery stores, gas stations and other retailers in my district, they talk about how they bear all of the costs for security breaches and fraud in the payment system – through interchange fees, chargebacks and penalties in the PCI contract.**

   When I talk with credit unions and community banks in my district, they talk about how they bear all the cost for data breaches and fraud in the payment system – costs for changing systems, reissuing cards, contacting customers etc – and never getting reimbursed for those expenses.

   If retailers are paying all this money in and the banks are bearing all of these costs, why isn't the money getting from the retailers to the banks? Can you

---

[2] Kenneth Olmstead and Aaron Smith, *Americans and Cybersecurity*, Pew Research Center (Jan. 26, 2017), available at http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

clarify what actually happens and why both my local retailers and community banks think they're getting the short end of the stick?

BSA Response:

The complex set of issues you've raised is unique to the relationship between the retail and financial services sectors. As a representative of an organization that advocates on behalf of the the enterprise software sector, I do not have professional insight into the questions you've raised.

QUESTIONS FOR THE RECORD
REP. DENNY HECK (WA-10)

Financial Institutions Subcommittee Hearing:
"Examining the Current Data Security and Breach Notification Regulatory Regime"

Hearing Date: February 14, 2018

Responses of Paul Rosenzweig
Senior Fellow, R Street Institute

1. **I have been trying to look into information on how many of the 145 million victims of the Equifax hack have had fake accounts opened in their name in the last several months, and there doesn't seem to be any public info on that.**

   a. **Does that exist? It seems like a spike of identity theft cases would be something we'd want to know quickly about so that people could freeze their credit or take other steps to protect themselves.**

      This information is not publicly collected in a single place that I am aware of. What little information we have does not suggest, however, that a spike in identity theft (i.e. actual fraud involving an known individual) has occurred.

   b. **Is this something that is publicly reported? Should it be?**

      This information is not currently publicly reported. Rather, however, than collect information on the misuse of personal information, I would support a reporting requirement that aggregated actual harm data, so that we had a better handle on the scope of the problem.

2. **One thing I heard in the aftermath of the Equifax breach was that it wasn't really that harmful on the margin because all of the information that was stolen in the breach was already available on the "dark web" anyway. Do you agree? I'm skeptical of these claims, but I'd like to hear your opinions.**

   Almost all personal data is available somewhere on the Dark Web. The difference in the Equifax breach is not in the quantum of information that is available but rather in the greater ease with which it can be accessed by malign actors. Thus, the statement is true, but it is not directly comparable.

3. **There are government agencies like the National Transportation Safety Board and Chemical Safety Board that are purely responsible for investigating and reporting on how disasters happen and what we can do to avoid them in the future.**

   I'm wondering about a Computer Network Safety Board that would investigate breaches like Equifax and issues reports on why the systems failed and how they could be made better. Is that an idea you think is worth exploring?

As I noted at the hearing, I think this is an idea worth exploring. It would need be structured so as to avoid creating incentives for non-cooperation (i.e. to avoid increasing liability) and it would also need to be structured so that it addresses both human and technical factors. But in the long run, we need to be able to "rate the risk" from cyber threats and having good data about how they occur is fundamentally a valuable exercise.

4. **When I meet with grocery stores, gas stations and other retailers in my district, they talk about how they bear all of the costs for security breaches and fraud in the payment system – through interchange fees, chargebacks and penalties in the PCI contract.**

   When I talk with credit unions and community banks in my district, they talk about how they bear all the cost for data breaches and fraud in the payment system – costs for changing systems, reissuing cards, contacting customers etc – and never getting reimbursed for those expenses.

   If retailers are paying all this money in and the banks are bearing all of these costs, why isn't the money getting from the retailers to the banks? Can you clarify what actually happens and why both my local retailers and community banks think they're getting the short end of the stick?

   The actual split of costs between retailers and banks is one that is the subject of great dispute and I have seen data supporting both positions.

   In the end, I think the dispute is really about rent-seeking – each group trying to off-load costs onto the other. The proper economic solution is to place responsibility on the least cost avoider – that is on the set of institutions that can mitigate the risks with the least amount of expenditure. While that, too, can be disputed it seems clear to this outsider that larger institutions with greater resources are typically in a better position both to improve security and to aggregate costs and distribute them.

   I would also note that that there are actually three types of entities at play here rather than two: the card issuer banks and the retailers identified in the question and also the card associations (Visa, Amex, Mastercard). The last of those three are probably in the best position to prevent fraud, since they are the smallest informational chokepoint and they get to see everything. That would tend to suggest that larger institutions, like card associations, should be the focus of our attention.

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

QUESTIONS FOR THE RECORD
REP. DENNY HECK (WA-10)

Financial Institutions Subcommittee Hearing:
"Examining the Current Data Security and Breach Notification Regulatory Regime"

Hearing Date: February 14, 2017

Responses of Marc Rotenberg,
President, Electronic Privacy Information Center (EPIC)

1. ***I have been trying to look into information on how many of the 145 million victims of the Equifax hack have had fake accounts opened in their name in the last several months, and there doesn't seem to be any public info on that.***

    a. ***Does that exist? It seems like a spike of identity theft cases would be something we'd want to know quickly about so that people could freeze their credit or take other steps to protect themselves.***

We agree that by this point, more detailed information should be available about the impact of the Equifax breach. While the Federal Trade Commission (FTC) reports aggregate data on identity theft, it has failed to do the necessary work to determine the precise connections between a data breach and the particular harm that results. That is one of the reasons EPIC has argued it is simply unfair to consumers to expect them to establish the causal connections between a breach and a harm. It is important to note also that evidence of physical crime—a broken door lock, a stolen laptop—is immediately apparent. But identity thieves often wait to make use of stolen credit card or bank account numbers, making it even more difficult for consumers to know when their personal data is at risk.

We would also call attention to the failure of the Consumer Financial Protection Bureau (CFPB) to pursue an effective investigation of the Equifax data breach. One year later, the CFPB has yet to issue any report or any fines. There were even reports that the CPFB had suspended the investigation entirely. That is extremely reckless behavior by a federal agency, particularly considering that the attack on the authenticating details of American consumers was coordinated by a foreign adversary.

b. Is this something that is publicly reported? Should it be?

Both the FTC and the CFPB should do more. More public information about identity theft would greatly aid consumers, investigators, and legislators. And more information should be known specifically about the Equifax breach.

2. ***One thing I heard in the aftermath of the Equifax breach was that it wasn't really that harmful on the margin because all of the information that was stolen in the breach was already available on the "dark web" anyway. Do you agree? I'm skeptical of these claims, but I'd like to hear your opinions.***

First, it should be clearly understood that the Equifax data breach was a targeted attack on the authenticating details of American consumers, launched by a foreign adversary. This was one of the greatest cyber attacks in the history of the United States, on par with the 2015 breach of OPM, which compromised the personal details of 22 million federal employees, their friends, and family members. To ignore the significance of the Equifax breach would be a grievous error.

And of course, major breaches such as the Equifax breach create additional harm to American consumers. Financial criminals regularly use the dark web to purchase and sell stolen private information.[1] While some criminals may obtain small amounts of information through direct attacks on individuals—such as spear phishing or skimming credit cards—more sophisticated criminals may perpetrate data breaches and other large-scale thefts to gain the information of millions at once. These attacks release millions of records to criminals in mere moments, leaving lasting harm and uncertainty to large swathes of the American public.

The sheer scale of the Equifax breach and the sensitivity of the data—the authenticating details that establish identity—is unparalleled. Significantly, the year following the breach saw the highest number of reported American identity theft victims on record.[2] More personal information available for improper use creates more opportunities for scammers and other criminals to steal and misuse American consumer information. And the loss of authenticating details compromises the integrity of all record systems, even beyond those primarily attacked.

3. ***There are government agencies like the National Transportation Safety Board and Chemical Safety Board that are purely responsible for investigating and reporting on how disasters happen and what we can do to avoid them in the future.***

I'm wondering about a Computer Network Safety Board that would investigate breaches like Equifax and issues reports on why the systems failed and how they could be made better. Is that an idea you think is worth exploring?

---

[1] *Cybercrime: The Threats*, INTERPOL, https://www.interpol.int/Crime-areas/Cybercrime/The-threats/The-Darknet.

[2] Robert N. Charette, *2017 Was a Record Year for ID Theft in the U.S.*, IEEE (Feb. 23, 2018), https://spectrum.ieee.org/riskfactor/computing/it/2017-is-another-us-record-year-in-id-information-thefts

Yes, the U.S. needs a Data Protection Agency. The United States is one of the few democracies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the U.S. in the 1970s.[3] The United States was once a global leader on privacy. The Fair Credit Reporting Act (FCRA), passed in 1970, was viewed at the time as the first modern privacy law—a response to the growing automation of personal data in the United States.[4]

Almost every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges faced by consumers and businesses. While often relied upon to police privacy, the Federal Trade Commission is fundamentally not a data privacy agency. The FTC only has authority to bring enforcement actions against unfair and deceptive practices, and lacks the ability to create forward-looking rules for data security. While the FTC does has limited data protection authority under the "Safeguards Rule" of the Gramm-Leach-Bliley Act (GLB), this rule only applies to financial institutions, and compliance is merely voluntary. Moreover, GLB disperses oversight of financial institutions across seven agencies and fails to cover credit reporting agencies, such as Equifax. Given that credit reporting agencies hold more sensitive personal data than many of the other financial institutions combined, it makes little sense for those companies to be given special treatment under the rules.

The Dodd-Frank Act transferred authority over certain privacy provisions of GLB to the Consumer Financial Protection Bureau, but Dodd-Frank did not give the CFPB authority to establish data security standards. The CFPB, like the FTC, can only bring enforcement actions based on a company's affirmative misrepresentations about data security practices. The CFPB similarly lacks data protection authority and only has jurisdiction over financial institutions. Neither of these agencies possess the resources needed to address data security.

As the data breach epidemic reaches unprecedented levels, the need for an effective, independent data protection agency has never been greater. An independent agency can more effectively utilize its resources to police the current widespread exploitation of consumers' personal information. An independent agency would also be staffed with personnel who possess the requisite expertise to regulate the field of data security.

EPIC would welcome the opportunity to work with the Committee to create a Data Protection Agency in the United States.

4. ***When I meet with grocery stores, gas stations and other retailers in my district, they talk about how they bear all of the costs for security breaches and fraud in the payment system — through interchange fees, chargebacks and penalties in the PCI contract.***

   When I talk with credit unions and community banks in my district, they talk about how they bear all the cost for data breaches and fraud in the payment system — costs for changing systems, reissuing cards, contacting customers etc

[3] *See*, EPIC, The Privacy Act of 1974, https://epic.org/privacy/1974act/#history.
[4] EPIC, *The Fair Credit Reporting Act*, https://www.epic.org/privacy/fcra/.

— ***and never getting reimbursed for those expenses.***

If retailers are paying all this money in and the banks are bearing all of these costs, why isn't the money getting from the retailers to the banks? Can you clarify what actually happens and why both my local retailers and community banks think they're getting the short end of the stick?

We are not familiar with the rules for the payment of fees between retailers and banks following a breach. So, we can offer no specific insight on this issue. However, to the extent that Congress is able to enact legislation that diminishes the likelihood of a data breach, we suspect the costs to both banks and retailers will be reduced.

Questions for All Witnesses:

1. I have been trying to look into information on how many of the 145 million victims of the Equifax hack have had fake accounts opened in their name in the last several months, and there doesn't seem to be any public info on that.

a. Does that exist? It seems like a spike of identity theft cases would be something we'd want to know quickly about so that people could freeze their credit or take other steps to protect themselves.

There is not a single repository for public information about fake accounts opened or attempted to be opened as a result of the Equifax breach. While we know what fake accounts have been attempted to be opened at our credit union we do not have public information about this from other financial institutions. Moreover, we must be cognizant of future identity theft attempts as a result of the breach. Litigation attorneys suing Equifax will seek to determine the full extent of the damages to consumers from the Equifax data breach.

b. Is this something that is publicly reported? Should it be?

It is likely that the credit reporting agencies have some statistics on identity theft and the genesis of these thefts. Public reporting could be helpful, but that would depend on the type of information made available to the public and, more importantly, that it would be actionable for consumers and business.

2. One thing I heard in the aftermath of the Equifax breach was that it wasn't really that harmful on the margin because all of the information that was stolen in the breach was already available on the "dark web" anyway. Do you agree? I'm skeptical of these claims, but I'd like to hear your opinions.

I strongly disagree with the statement. It may be possible to pick a person and use many resources to find information about that person for an attempted identity theft or fraud, but the quantity and quality of information available is highly variable. Equifax and other Credit Reporting Agencies house almost every bit of important personal financial information on a consumer. Their information runs so deep that it is often used to identify consumers because the reporting agencies have information that only a consumer is likely to know. For example, whether a financial institution holds a loan on a 1999 Toyota truck. This very type of information is often used to identify or verify the consumer in the first instance.

3. There are government agencies like the National Transportation Safety Board and Chemical Safety Board that are purely responsible for investigating and reporting on how disasters happen and what we can do to avoid them in the future.

I'm wondering about a Computer Network Safety Board that would investigate breaches like Equifax and issues reports on why the systems failed and how they could be made better. Is that an idea you think is worth exploring?

I believe a question like this was posed to the panel during the testimony session. It seems that these massive data breaches, although criminal, also represent a threat to national security. The Department of Homeland Security can and probably should have a role investigating large and important data breaches. That said, there may be a role for an agency focuses merely on the mechanics of a data breach and how to prevent them. It's important to remember that some of the largest data breaches involved a lack of basic computer hygiene, such as updating software for known vulnerabilities, or storing information that should not have been stored in the first place. What an agency would not be equipped to do is compensate victims for the harm from the data

breach that was the result of a company's own negligence in preventing the breach from occurring, and therefore, any such investigatory body should not limit the right of victims to seek redress.

4. When I meet with grocery stores, gas stations and other retailers in my district, they talk about how they bear all of the costs for security breaches and fraud in the payment system – through interchange fees, chargebacks and penalties in the PCI contract.

When I talk with credit unions and community banks in my district, they talk about how they bear all the cost for data breaches and fraud in the payment system – costs for changing systems, reissuing cards, contacting customers etc – and never getting reimbursed for those expenses.

If retailers are paying all this money in and the banks are bearing all of these costs, why isn't the money getting from the retailers to the banks? Can you clarify what actually happens and why both my local retailers and community banks think they're getting the short end of the stick?

Financial institutions and retailers may be responsible, but there are large differences in the scope of responsibility. Retailers are only responsible for fraud at the point of sale in very limited circumstances. An example of this could be when a retailer accepts a credit transaction using the mag stripe (swiping the card) when the card has an EMV chip or through online transactions. Mainly, these are transactions when the retailer should have known a transaction was fraudulent and could have prevented by adopting the latest standards. It should be noted that financial institutions still bear the brunt of these expenses because network rules don't allow chargebacks over a certain size.

Financial institutions on the other hand are responsible for all fraud reimbursement and functionally act as an insurer. When a retailer is breached and loses card data or loses card data in any other way, a financial institution is responsible for the fraud costs that follow. This includes all fraud purchases made with the card, card reissuances, fraud monitoring systems, and legal costs. One member credit card can cost thousands of dollars in fraud. Multiply that by an entire breach and it now cost us hundreds of thousands. Interchange helps support the debit and credit process as delivery of payments, whether it be cash, checks. All of these payment methods have costs. Fraud costs are on top of that.

The problem with breaches is that they often result in large losses that leave financial institution vulnerable with little ability to protect themselves or consumers.

The card networks also have some rules in place that provide for some limited reimbursement to financial institutions from retailers for breach. These rules provide for pennies on the dollar and are generally only applicable to the larger breaches of larger institutions. In the case of Wendy's, it is highly likely that financial institutions will not be reimbursed through this process because stores are owned by franchisees even though point of sale system breached was owned and operated by corporate Wendy's.

The bottom line is that retailers can be responsible for certain breach related costs, but only when the fraud was preventable and retailers often are able to shift the liability when they complied with their contractual obligations. Financial institutions are responsible for many types fraud, most of which they cannot prevent nor did they have any responsibility in creating.

It should also be noted that VISA rules, as part of their contract with merchants, often times prohibit merchants from storing personal information but these rules are regularly ignored by the merchants and VISA does not take enforcement action.

The small merchant is not hurt by the regulatory requirements we are proposing because they work with a processor that would be responsible for ensuring data protection like "Square" for example.

Without requirements to protect consumer data IF the company holds the data, consumers are left at the whim of the company's data security. Consumers have no way of knowing the diligence of the company's data protection and is left subject to breaches that may cost them their entire life savings from being an identity fraud victim.

QUESTIONS FOR THE RECORD
REP. DENNY HECK (WA-10)

Financial Institutions Subcommittee Hearing:
"Examining the Current Data Security and Breach Notification Regulatory Regime"

Hearing Date: February 14, 2018

Below are the response of Nathan Taylor, Partner at Morrison & Foerster LLP to the following Questions for the Record.

Questions for All Witnesses:

1. I have been trying to look into information on how many of the 145 million victims of the Equifax hack have had fake accounts opened in their name in the last several months, and there doesn't seem to be any public info on that.

    a. Does that exist? It seems like a spike of identity theft cases would be something we'd want to know quickly about so that people could freeze their credit or take other steps to protect themselves.

    b. Is this something that is publicly reported? Should it be?

    I cannot speak to the Equifax breach specifically. Nonetheless, I am happy to provide general comments based on my work representing companies with respect to cybersecurity issues.

    For any given breach involving Social Security numbers ("SSNs"), I do not believe that it is possible to track the extent to which those SSNs have been used, if at all, along with other information to open fraudulent accounts in the victims' names (*i.e.*, to commit identity theft). I believe this to be true for a number of reasons, including the following.

    There are numerous forms of potential identity theft in which a fraudster may provide a stolen SSN in connection with the fraudster's effort to perpetrate the fraudulent act. For example, identity theft involving SSNs can include fraudulently obtaining a financial product or service (*e.g.*, opening a credit card), establishing a cell phone plan or utility connection, submitting fraudulent tax returns, committing insurance or health care related fraud and obtaining a fraudulent civil judgment, to name just a few. Because the types of identity theft vary significantly, it goes without saying that the companies (and even government agencies) that are also the victims of identity theft are countless. In my view, it likely would be impossible to gather credible statistics from all companies (and many government agencies) in America to capture every incident of identity theft (regardless of its source).

    Even if a rough estimate of the national occurrence of identity theft involving SSNs could be obtained, it is not clear how the ultimate "cause" of the identity theft could be determined in many, if not most, cases. In this regard, data breaches involving SSNs are certainly one cause. But there are others, including unwitting victims providing their information to fraudsters, physical thefts of documents and devices, malware on consumer computers (*e.g.*, keyloggers) and instances in which the fraudster is a family member or close acquaintance of the victim.

Finally and most importantly, it is not clear to me how the causal link could be established tying any given occurrence of identity theft to a specific breach. As discussed below in my response to Question 2, there are numerous breaches involving SSNs, including those that are discovered and publicly reported by companies, those that are discovered and never reported and those that are simply never discovered. I'm not aware of any acknowledged method to prove the causal link between a breach involving SSNs and the resulting identity theft. This challenge is of course exacerbated by the fact that the volume of consumer information available for sale by criminals (often obtained from breaches) has exponentially multiplied over the years.

I appreciate that the question appears focused on alerting consumers to increased spikes in identity theft so that they can take to protect themselves from harm. In my view, requiring prompt breach notification, as well as consumer education about the need to always be vigilant and take steps to monitor and protect yourself (*e.g.*, regularly reviewing free credit reports and filing security freezes), is a far better option to trying to track the correlation of identity theft to specific breaches in order to alert consumers. In this regard, it is the breach notification itself which functions as the alert. That is its very purpose.

2. One thing I heard in the aftermath of the Equifax breach was that it wasn't really that harmful on the margin because all of the information that was stolen in the breach was already available on the "dark web" anyway. Do you agree? I'm skeptical of these claims, but I'd like to hear your opinions.

I cannot speak to the Equifax breach specifically. Nonetheless, I am happy to provide general comments based on my work representing companies on cybersecurity issues.

For any given breach involving SSNs, the "marginal" increased risk of identity theft will depend on a number of factors, many of which a consumer would not be able to determine. As a consumer, I have received notices of breaches involving my SSN on a number of occasions. As a result, I am confident that my SSN is available to potential fraudsters, such as on the dark web. Nonetheless, the fact that it is likely available today does not quantify the potential risk of a breach involving my SSN tomorrow. In this regard, the actual risk associated with the next breach involving my SSN will depend entirely on the facts surrounding that breach.

As I indicated in my testimony, breaches are not created equally. They come in many forms. For example, a breach could involve anything from an inadvertent disclosure to a trusted or an unknown third party, a complex nation state attack to hackers motivated by potential gain. In this regard, the attacker's motivation may be the largest driver of risk to the consumer. Take two examples involving the same types of facts: either a nation state actor or a hacker compromises a company's systems and is able to identify a trove of consumer information, including my name and SSN, and then successfully exfiltrate and steal that information. If the nation state actor has conducted the attack for political or intelligence purposes because the nation state has identified value in the information to support its purposes, the risk to me of identity theft as a result of the breach may in fact be limited. If the bad actor is a hacker motivated by potential financial gain, the exact opposite may be true; that is, in this latter scenario, I may be at significant risk of identity theft, either because the actor may use the

information to attempt to open a fraudulent account in my name or, more likely, sell the information to third parties who will then make such attempts.

As a consumer who has received a number of notices of breaches involving my SSN (among other information), including, for example, the Office of Personnel Management ("OPM") breach, it is typically impossible for me to know the salient facts, including, among others, the identity of the attacker, what the attacker's motivation was/is and what the attacker has done with the information since the attack (*e.g.*, sold the information to others). As a result, as a consumer, the only reasonable assumption that I can make when I receive the next letter regarding a breach involving a malicious actor (as opposed to, for example, an accidental or inadvertent disclosure in which there may be low risk of harm) is to assume that I am at risk of identity theft. And, the fact that my SSN was previously involved in, for example, the OPM breach among others has no bearing on whether the attacker in the next breach may attempt identity theft in my name.

3. There are government agencies like the National Transportation Safety Board and Chemical Safety Board that are purely responsible for investigating and reporting on how disasters happen and what we can do to avoid them in the future.

   I'm wondering about a Computer Network Safety Board that would investigate breaches like Equifax and issues reports on why the systems failed and how they could be made better. Is that an idea you think is worth exploring?

Your question is an intriguing one, and one that I have thought about since you first raised the issue during the hearing. While I think there are a number of practical challenges that the government would face in the successful implementation of a Computer Network Safety Board ("Board"), I think it is reasonable that the broader data security debate that Congress is continuing should include discussion about the concept.

In my view, however, we already have today the functional equivalent of a Board, at least for high-profile breaches. More specifically, for a high-profile breach, it is typical for a host of federal and state regulatory and other government bodies to conduct investigations regarding the breach, often resulting in enforcement actions. For example, the Federal Trade Commission, the state Attorneys General, the Securities and Exchange Commission, both Houses of the U.S. Congress, and other federal and state regulators (*e.g.*, the federal banking agencies) frequently conduct investigations of high-profile breaches. However, it is worth noting that despite the significant number of breach-related investigations that are conducted by regulators, the various regulators do not consistently provide guidance to companies regarding lessons learned and steps that companies can take to avoid similar breaches.

In my view, a reasonable alternative to the Board concept would be to have legislation establishing a uniform, national standard for data security that is enforced primarily by a single federal regulator, such as the Federal Trade Commission. That legislation could also require that the federal regulator periodically provide guidance to companies regarding security issues that the agency has identified in breach investigations. I note that this occurs today at least in the sense that companies can look to, for example, Federal Trade Commission and state Attorneys General enforcement actions to identify practices that these enforcement agencies believe are not reasonable.

Finally, I would highlight some of the practical challenges associated with creating such a Board. First, how would Congress create standards to guide which breaches the Board would investigate? Data breaches are quite distinct from, for example, plane crashes, nuclear incidents and oil spills from a sheer volume perspective. While other federal boards may only need to investigate tens or even hundreds of incidents on an annual basis, there are thousands of publicly reported breaches each year. Related to this volume issue, how would Congress fund such a Board?

4. When I meet with grocery stores, gas stations and other retailers in my district, they talk about how they bear all of the costs for security breaches and fraud in the payment system – through interchange fees, chargebacks and penalties in the PCI contract.

When I talk with credit unions and community banks in my district, they talk about how they bear all the cost for data breaches and fraud in the payment system – costs for changing systems, reissuing cards, contacting customers etc – and never getting reimbursed for those expenses.

If retailers are paying all this money in and the banks are bearing all of these costs, why isn't the money getting from the retailers to the banks? Can you clarify what actually happens and why both my local retailers and community banks think they're getting the short end of the stick?

Your question (and the feedback that you have received from your constituents) highlights the complexity surrounding the issue of "costs" and "losses" resulting from a retailer's breach involving payment card information. In particular, it highlights the fact that in breaches involving payment cards, there are no winners. The following response is based on my understanding of how the payment card network breach recovery process generally works. Of course, the breach recovery process differs from network to network. In addition, this recovery process is only one avenue through which a bank may recover costs associated with a payment card breach; for example, the following does not address litigation between banks and retailers.

As I understand it, payment card networks typically have programs designed to allow card issuers to recover some portion of costs resulting from certain large-scale payment card breaches that involve the retailer's failure to comply with the Payment Card Industry Data Security Standard ("PCI DSS"). In these instances, the payment card network may levy an assessment against the retailer's merchant acquiring bank. In many cases, the merchant acquiring bank will seek indemnification from the retailer for the assessment.

The purpose of the assessment is to recover at least a portion of relevant card issuer operational costs resulting from the breach, such as the costs of reissuing payment cards. The assessment is unlikely to cover an issuer's actual operational costs, instead covering only a percentage. In addition, the assessment may not cover any of an issuer's fraud losses. Nonetheless, the payment card network will then provide the funds from the assessment to the relevant card issuers.

It is also worth noting that, for many smaller-scale payment card breaches, the retailer's merchant acquiring bank will not receive an assessment from the payment card

networks and the relevant issuers will not receive any reimbursement through the payment card network breach recovery process.

○