

# WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?

---

## HEARING BEFORE THE SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS FIRST SESSION

JANUARY 27, 2015

**Serial No. 114-4**



Printed for the use of the Committee on Energy and Commerce  
*energycommerce.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

20-396 PDF

WASHINGTON : 2016

---

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

## COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan

*Chairman*

JOE BARTON, Texas

*Chairman Emeritus*

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOSEPH R. PITTS, Pennsylvania

GREG WALDEN, Oregon

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

*Vice Chairman*

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. McKINLEY, West Virginia

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

RENEE L. ELLMERS, North Carolina

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

FRANK PALLONE, Jr., New Jersey

*Ranking Member*

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

LOIS CAPPS, California

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

JOHN A. YARMUTH, Kentucky

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

---

## SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MICHAEL C. BURGESS, Texas

*Chairman*

LEONARD LANCE, New Jersey

*Vice Chairman*

MARSHA BLACKBURN, Tennessee

GREGG HARPER, Mississippi

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

GUS M. BILIRAKIS, Florida

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

FRED UPTON, Michigan (*ex officio*)

JANICE D. SCHAKOWSKY, Illinois

*Ranking Member*

YVETTE D. CLARKE, New York

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

BOBBY L. RUSH, Illinois

G.K. BUTTERFIELD, North Carolina

PETER WELCH, Vermont

FRANK PALLONE, Jr., New Jersey (*ex officio*)

## C O N T E N T S

	Page
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement .....	2
Prepared statement .....	3
Hon. Leonard Lance, a Representative in Congress from the State of New Jersey, opening statement .....	4
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement .....	5
Prepared statement .....	6
Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement .....	8
Prepared statement .....	8
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement .....	10
Prepared statement .....	11

### WITNESSES

Elizabeth Hyman, Executive Vice President, Public Policy, TechAmerica, Computing Technology Industry Association .....	12
Prepared statement .....	15
Answers to submitted questions .....	97
Brian A. Dodge, Executive Vice President, Communications and Strategic Initiatives, Retail Industry Leaders Association .....	26
Prepared statement .....	28
Answers to submitted questions <sup>1</sup> .....	102
Jennifer Barrett-Glasgow, Global Privacy Officer, Acxiom Corporation .....	34
Prepared statement .....	36
Answers to submitted questions .....	103
Woodrow Hartzog, Associate Professor of Law, Cumberland School of Law, Samford University .....	43
Prepared statement .....	45
Answers to submitted questions .....	108

### SUBMITTED MATERIAL

Letter of January 27, 2015, from Gary Shapiro, President and Chief Executive Officer, Consumer Electronics Association, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	74
Letter of January 26, 2015, from Peggy Hudson, Senior Vice President, Government Affairs, Direct Marketing Association, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	76
Letter of January 23, 2015, from American Bankers Association, et al., to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	78
Letter of January 26, 2015, from Howard Fienberg, Director of Government Affairs, Marketing Research Association, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	80
Letter of January 27, 2015, from David French, Senior Vice President, Government Relations, National Retail Federation, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	81
Letter of January 23, 2015, from Carrie R. Hunt, Senior Vice President of Government Affairs and General Counsel, National Association of Federal Credit Unions, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	83

<sup>1</sup> Mr. Dodge did not answer submitted questions for the record by the time of printing.

IV

	Page
Letter of January 27, 2015, from Consumer Data Industry Association, et al., to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	86
Statement of National Association of Convenience Stores and Society of Independent Gasoline Marketers of America, January 27, 2015, submitted by Mr. Burgess .....	88

## WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?

TUESDAY, JANUARY 27, 2015

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND  
TRADE,  
COMMITTEE ON ENERGY AND COMMERCE,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 11:06 a.m., in room 2123 of the Rayburn House Office Building, Hon. Michael C. Burgess (chairman of the subcommittee) presiding.

Members present: Representatives Burgess, Lance, Blackburn, Harper, Guthrie, Olson, Kinzinger, Bilirakis, Mullin, Upton (ex officio), Schakowsky, Clarke, Kennedy, Cárdenas, Rush, Butterfield, Welch, and Pallone (ex officio).

Staff present: Charlotte Baker, Deputy Communications Director; Leighton Brown, Press Assistant; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Kirby Howard, Legislative Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Olivia Trusty, Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Counsel, Commerce, Manufacturing, and Trade; Jeff Carroll, Democratic Staff Director; Lisa Goldman, Democratic Counsel, Commerce, Manufacturing, and Trade; Tiffany Guarascio, Democratic Deputy Staff Director; and Meredith Jones, Democratic Director of Outreach and Member Services.

Mr. BURGESS. Well, good morning, everyone. Before we begin our first subcommittee meeting of the 114th Congress, the ranking member and I would like to briefly recognize new members of the subcommittee. For the benefit of the ranking member, I am not a new member. I was on this subcommittee several terms ago. So I am back on the subcommittee. For that I am grateful, but on the majority side—I don't believe she has joined us yet—but we have Ms. Brooks representing the 5th District of Indiana and Mr. Markwayne Mullin representing Oklahoma's 2nd District. Welcome to the committee, welcome to the subcommittee. We are grateful and excited to have you on board. For the minority, Subcommittee Ranking Member Schakowsky will introduce her new members.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, for just letting me say how much I look forward to working with you on this subcommittee. New members include Yvette Clarke. She represents New York's 9th Congressional District as a proud Brooklyn native with strong roots planted in her Jamaican heritage. She is an out-

spoken advocate for her district, always working to champion the middle class and those who aspire to reach it. Her district has become a center of innovation for health care and includes some of the best hospitals, trade associations, and businesses in the industry. I look forward to her bringing her tenacity, deep knowledge, and enthusiasm to this subcommittee.

Next to her is Joe Kennedy, who serves the people of Massachusetts' 4th, has dedicated his life to public service, and brings with him a firm commitment to social justice and economic opportunity. Joe has previously served in the Peace Corps, worked as an International Development Analyst for the United Nations' Millennium Project, and as an anti-poverty consultant abroad. I know that he will bring that passion for public service and economic growth to everything he does on the subcommittee. And not here now but also a new member of the subcommittee is Tony Cárdenas representing California's 29th Congressional District. He has made a name for himself by always advocating strongly on behalf of his constituents on issues like juvenile justice, immigration, higher education, and economic improvement. He has brought hard work and dedication to his 16 years of public service on behalf of the people of the Northeast San Fernando Valley. As a former small business owner, an engineer, head of the California Budget Committee, and as a leader in environmental progress in the City of Los Angeles, I am certain Tony will be able to lead his expertise to our subcommittee's progress. Thank you, Mr. Chairman.

Mr. BURGESS. Thank you, Ranking Member Schakowsky. We welcome all members of the subcommittee back and look forward to working with each and every one of you in the 114th Congress.

Before I get started, I also want to recognize a visiting delegation of the legislative staff from the Parliaments of Georgia, Kosovo, Macedonia, and Nepal through the House Democracy Partnership. They are in town for a seminar on strengthening committee operations and are observing today's hearing as part of the program. I hope they are able to learn a great deal, both today and during their tenure here the rest of the week.

Ms. SCHAKOWSKY. Mr. Chairman, could they acknowledge themselves so we can all see who they are. Great. Thank you.

Mr. BURGESS. Welcome. Thank you for coming. I am glad you were able to make it here with the weather.

The Subcommittee on Commerce, Manufacturing, and Trade will now come to order. I will recognize myself for 5 minutes for the purposes of an opening statement.

#### **OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS**

The purpose of today's hearing is to move one step closer to a single, Federal standard on data security and breach notification. Increasingly, our personal details, which we need to verify financial transactions, are converted into data and uploaded to networks of servers, and not always can those servers be protected with a simple lock and key. We benefit immensely from the quick access and command this system gives us. Global commerce is literally at our fingertips on a daily basis.

And yet such a dynamic environment brings with it dynamic, evolving risks. As our options multiply, so must our defensive measures. Those defensive measures must adapt quickly. As several commentators have noted in testimony before this subcommittee, it is no longer a matter of if a breach occurs. It is when and what happens when.

Even so, questions remain as to whether businesses are doing enough to prevent security breaches. That is why I believe Federal legislation should include a single but flexible data security requirement. Now, about 12 States have already implemented such a requirement on commercial actors that are not banks or health care providers.

A single requirement across the States would give companies some confidence that their methods are sound in handling electronic data, an inherently interstate activity. Moreover, it would put all companies on notice that if you fail to keep up with other companies, if you aren't learning from other breaches, you will be subject to Federal enforcement.

Indeed, too many resources are spent trying to understand the legal obligations involved with data security and breach notification. Certainty would allow those resources to be spent on actual security measures and notifications and their affected consumers.

As we discuss the necessary elements of a data breach bill, there are a few considerations that I want to mention. First, there is a limited window for us to act. Criminal data breaches have grabbed the headlines for about a decade, but a consensus solution has thus far eluded Federal legislators. This committee is calling for action, the President asked for legislation with national breach notification, and the Senate has legislation in front of it with a national standard.

But most importantly, it is our consumers who are calling for legislation, thus giving us the time to act.

Second, this legislation is limited to this committee's jurisdiction. The surest way to deny consumers the benefits of Federal data security legislation is to go into areas beyond our jurisdiction. Specifically, the health care and the financial sectors have their own regimes. If we aim to rewrite rules for those sectors, then it will be years, perhaps decades, before a bill is signed into law. That is not to say that we will ignore those issues. But they may need to be taken up separately.

Third, our aspiration at this point is that legislation comes forward with bipartisan support, and do sincerely believe that that is an achievable goal.

With this hearing, I aim to understand the policy points where stakeholder compromise is possible. We are seeking to find agreement not only between the two sides of the dais but also between stakeholders with divergent interests. The sooner we understand the most important principles, the smoother negotiations will go over the next several months.

[The prepared statement of Mr. Burgess follows:]

#### PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

The purpose of today's hearing is to move one step closer to a single, Federal standard on data security and breach notification.

Increasingly, our personal details—which we need to verify financial transactions—are converted into data and uploaded to networks of servers that can’t be protected with a simple lock and key.

We benefit immensely from the quick access and command this system gives us—the world’s merchants are at our fingertips.

And yet such a dynamic environment brings with it a dynamic and evolving set of risks. As our options multiply, so must our defensive measures.

Those defensive measures must adapt quickly. As several commentators have noted in testimony before this subcommittee, it is no longer a matter of if a breach occurs, but when.

Even so, questions remain as to whether businesses are doing enough to prevent security breaches.

This is why I believe Federal legislation should include a single-but flexible-data security requirement. Now, about 12 States have already implemented such a requirement on commercial actors that are not banks or health care providers.

A single requirement across the States would give companies some confidence that their methods are sound in handling electronic data, an inherently interstate activity.

Moreover, it would put all companies on notice that if you fail to keep up with other companies and if you aren’t learning from other breaches, you will be subject to Federal enforcement.

Indeed, too many resources are spent trying to understand the legal obligations involved with data security and breach notification. Certainty would allow those resources to be spent on actual security measures and notifications to affected consumers.

As we discuss the necessary elements of a data breach bill, there are a few considerations I want to mention.

First, there is a limited window for us to act. Criminal data breaches have grabbed headlines for about a decade, but a consensus solution has thus far eluded Federal legislators.

This committee is calling for action, the President is calling for legislation with a national breach notification regime, and the Senate has legislation with a national standard. But most importantly, consumers are calling for legislation—the time to act is now.

Second, this legislation is limited to this committee’s jurisdiction; the surest way to deny consumers the benefits of Federal data security legislation is to visit areas beyond our jurisdiction.

Specifically, the healthcare and financial sectors have their own regimes. If we aim to rewrite rules for those sectors then it will be years before a bill is signed into law.

That is not to say that we will ignore those issues. But they may need to be taken up separately. Third, our aspiration at this point is for legislation with bipartisan support and I believe that is achievable.

With this hearing, I aim to understand the policy points where stakeholder compromise is possible. We are seeking to find agreement not only between the two sides of the aisle, but also between stakeholders with divergent interests.

The sooner we understand the very most important principles, the smoother negotiations will go over the next couple months.

Mr. BURGESS. With that, I do want to thank our witnesses for the testimonies that they have provided us and representing their interests candidly in the spirit of compromise. And I would like to recognize the vice chair of the subcommittee, Mr. Leonard Lance of New Jersey.

**OPENING STATEMENT OF HON. LEONARD LANCE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY**

Mr. LANCE. Thank you, Mr. Chairman, and it is an honor to serve under your leadership as the new chair of the subcommittee, and I am sure you will do a superb job.

Well, the debate over data breach legislation has continued for several years. The issue has been brought to the forefront by unfor-



fortunate, high-profile breaches recently, and of course, the most recent is the Sony Pictures hack at the end of last year.

The question of how to proceed on data breach reform has wide implications for both businesses and consumers alike. Today businesses that attempt to report a breach must navigate through a complex labyrinth of 47 State laws which are not all the same. Each State has answered the following questions in its own way: What is defined as an event trigger? What is the appropriate time-frame by which companies must notify consumers that their identifiable information has been breached? Who is responsible for notifying affected consumers?

The lack of certainty of these regulations places an undue burden on businesses trying to report a breach properly and an undue burden on consumers. Federal law will streamline regulations, give certainty to businesses resulting in greater compliance and also to consumers who suffer a data breach.

However, it is my belief that it will only be effective if it preempts the patchwork of 47 State laws. The debate over Federal data breach legislation has continued over the span of several Congresses. It is my hope that we can pass effective, bipartisan data breach legislation this year.

Thank you, Mr. Chairman.

Mr. BURGESS. The Chair thanks the gentleman. The Chair now recognizes the subcommittee ranking member, Ms. Schakowsky, for 5 minutes for the purpose of an opening statement.

**OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS**

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, for holding today's important hearing on what to include in Federal legislative approach to the challenges of data security and breach notification.

I look forward to our work together in the 114th Congress, and this is a great issue to open up with.

Data security is one of the most important issues that this subcommittee will consider this year. In the State of the Union last week, the President urged us to pass legislation that will better protect against cyberattacks and identity theft. I look forward to working with the White House and my colleagues on both sides of the aisle to meet that goal.

Since 2005, over 900 million records with personally identifiable information have been compromised. The recent uptick in high-profile data breaches including those of Target, Home Depot, Neiman Marcus, and Michael's prove two important points: One, just about every retailer and many nonretailers that we engage with are collecting and storing our personal information, credit card numbers, contact information, and much more. And two, hackers are growing in number and becoming more sophisticated in their attempts to access that personal information, and they are having more success. From programming home security systems and thermostats from hundreds of miles away, to remembering shopping preferences and account information, to connecting with friends over the Internet, Americans benefit in many ways from an increasingly data-driven world. But that doesn't mean we should sacrifice our right

to have our personal information appropriately protected or our right to know if and when that data has been compromised.

There are a variety of State laws regarding data security standards and breach notification requirements. However, there is no comprehensive Federal standard for appropriate protection of personally identifiable information, nor are there Federal requirements in place to report data breaches to those whose personal information has been exposed. And I firmly believe that legislation to address that data breach threat must include those two safeguards.

It is important to say that no legislation to require data security standards and breach notification will completely eliminate the threat of data breach. That being said, entities that collect and store personal information must take reasonable steps to protect data, and consumers must be informed promptly in the event of a breach.

And while I clearly believe that the Federal Government should have a role in data breach—that is what we have been working toward—I also believe that there have been many important protections that are at the State level that we don’t want to eliminate when we do Federal legislation, perhaps even eliminating rights and protections that would not be guaranteed under Federal statute. We have to be sure that we don’t weaken protections that consumers expect and deserve. If we include Federal preemption of some of those things or if we don’t include those good things in Federal legislation, then I think that would be a serious mistake at this point.

I also believe that if we include Federal preemption, we must ensure that State Attorneys General are able to enforce the law, something my Attorney General has made very, very clear.

So I think we can achieve all these goals working together, get a good, strong Federal bill that makes consumers feel confident that we have taken the appropriate steps.

[The prepared statement of Ms. Schakowsky follows:]

#### PREPARED STATEMENT OF HON. JANICE D. SCHAKOWSKY

Thank you, Mr. Chairman, for holding today’s important hearing on what to include in a Federal legislative approach to the challenges of data security and breach notification. I look forward to our work together in the 114th Congress, and this is a great issue to open with.

Data security is one of the most important issues that this subcommittee will consider this year. In the State of the Union last week, the President urged us to pass legislation that will better protect against cyberattacks and identity theft. I look forward to working with the White House and my colleagues on both sides of the aisle to meet that goal.

Since 2005, over 900 million records with personally identifiable information have been compromised. The recent uptick in high profile data breaches—including those of Target, Home Depot, Neiman Marcus, and Michael’s—proves two important points:

1. Just about every retailer—and many nonretailers—that we engage with are collecting and storing our personal information—credit card numbers, contact information, and much more.
2. Hackers are growing in number and becoming more sophisticated in their attempts to access that personal information—and they are having more success.

From programming home security systems and thermostats from hundreds of miles away to remembering shopping preferences and account information to connecting friends over the Internet, Americans benefit in many ways from an increasingly data-driven world. But that doesn’t mean we should sacrifice our right to have

our personal information appropriately protected, or our right to know if and when that data has been compromised.

There are a variety of State laws regarding data security standards and breach notification requirements. However, there are no comprehensive Federal standards for appropriate protection of personally identifiable information. Nor are there Federal requirements in place to report data breaches to those whose personal information has been exposed. I firmly believe that legislation to address the data breach threat must include those two safeguards.

It is important to say that no legislation to require data security standards and breach notification will completely eliminate the threat of data breach. That being said, entities that collect and store personal information must take reasonable steps to protect data, and consumers must be informed promptly in the event of a breach.

While I clearly believe the Federal Government should have a role on data breach, I am concerned about the impacts of Federal legislation that would pre-empt State law. Federal preemption could weaken important consumer protections—perhaps even eliminating rights and protections that would not be guaranteed under a Federal statute. We must be sure not to weaken the protections consumers expect and deserve. If we include Federal preemption, we must ensure that State Attorneys General are able to enforce the law.

I look forward to hearing the views and perspectives of our panel on the Federal role in this important issue. I yield back the balance of my time.

Ms. SCHAKOWSKY. And let me with my remaining time yield to Peter Welch for his comments.

Mr. WELCH. Thank you very much. Mr. Chairman and Ranking Member, you both nailed it with your description of what we are doing. It is pretty astonishing that with the use of computers, two things still have not been done at the Federal level: one, to provide data breach security, and number two, to provide notice to consumers. Consumers receive notice when they have been harmed, but they don't need notice just to scare them. And we have bipartisan momentum here, thanks to Chairman Upton and my colleague Marsha Blackburn, who I have been working with, and Congressman Rush has been working on this for a long time. So we have got a foundation here.

The practical challenges, those are the ones we have to resolve. What do we do about a national standard? What do we do about having enforcement at the AG level, something I agree with Ms. Schakowsky on. What is the notice standard? When should consumers be notified? How do you give some time for a company that has been breached to do law enforcement, investigation, and inquiry into what the scope of the breach was? These are more or less practical issues. And I think the chairman has set a good tone here where we have a common objective, and we don't have ideological differences. We have practical differences. And the hope I think of all of us with the foundation that has been laid by my predecessors is to find some common-sense, legitimate balancing of the interests so that at the end of the day we do protect consumers with data breach security, we give some reasonable certainty to our companies, and we have a standard that is robust and strong. I yield back.

Mr. BURGESS. I thank the gentleman. The gentleman yields back. The Chair now recognizes the chairman of the full committee, Mr. Upton, for 5 minutes for an opening statement.

**OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN**

Mr. UPTON. Thank you, Mr. Chairman, and it has been noted this committee does have a strong tradition of bipartisan cooperation and problem solving. In this spirit, today we continue our focus on the key elements to pass a Federal data breach law, a priority that the President identified in his State of the Union address just last week. I look forward to working with the White House, Dr. Burgess, and members of this committee on both sides of the aisle to accomplish that goal.

Criminal cyberhacking presents a serious risk of economic harm to consumers and businesses alike. From small mom-and-pop shops in my district in Southwest Michigan to global Fortune 100 companies, the unfortunate reality is that companies of all sizes are at risk of having information hacked.

This committee will be examining a series of issues relating to cybersecurity in this Congress. Where the conversation begins today is with a data breach bill, and I want to encourage all members and the public to focus on getting that issue right before we try to tackle some of the other concerns. There are significant privacy issues in an online economy, and some of those will have to be addressed separately.

Let us also be clear that this isn't a financial services bill. We cannot let data breach legislation be sunk by extraneous issues.

Today's hearing will examine two discrete issues related to the complex effects of cybercrime, commercial data security and breach notification to consumers. There is a real opportunity this Congress to set a single, national standard for data security and breach notification. I personally believe that a single, Federal standard is the key to passing a solution. The trade-off is that it has to be a strong, consumer-friendly law, one that has real protections and real enforcement. Both the FTC and State AGs have shown that this is an area that they would police very effectively. Our role is to strike the right balance on when notification is required, how timely it needs to be, and what information leads to identity theft.

Setting a national standard benefits consumers by ensuring that every business must look at their activities and make certain that they are taking reasonable security measures. A national standard allows businesses to focus on securing information and systems instead of trying to figure out how to comply with a host of different State laws with their team of lawyers. Consumers benefit from consistency as well.

We are particularly concerned with the impact that these criminal acts have on consumer confidence, economic growth, and job creation. So let us get to work. A data breach bill is the first step in securing that future.

[The prepared statement of Mr. Upton follows:]

**PREPARED STATEMENT OF HON. FRED UPTON**

This committee has a strong tradition of bipartisan cooperation and problem solving. In this spirit, today we continue our focus on the key elements to pass a Federal data breach law—a priority the president identified in his State of the Union address last week. I look forward to working with the White House, Dr. Burgess, and members of this committee to accomplish that goal.

Criminal cyberhacking presents a serious risk of economic harm to consumers and businesses alike. From small mom-and-pop shops in Southwest Michigan to global fortune 100 companies—the unfortunate reality is that companies of all sizes are at risk of having information hacked.

This committee will be examining a series of issues relating to cybersecurity this new Congress. Where the conversation begins today is with a data breach bill, and I want to encourage members and the public to focus on getting that issue right before we try to tackle some of the other concerns. There are significant privacy issues in an online economy, and some of those will have to be addressed separately. Let's also be clear that this isn't a financial services bill. We cannot let data breach legislation be sunk by extraneous issues.

Today's hearing will examine two discrete issues related to the complex effects of cybercrime: commercial data security and breach notification to consumers. There is a real opportunity this Congress to set a single, national standard for data security and breach notification.

I personally believe that a single, Federal standard is the key to passing a solution. The trade-off is that it has to be a strong, consumer-friendly law—one that has real protections and real enforcement. Both the FTC and State AGs have shown that this is an area that they would police very effectively. Our role is to strike the right balance on when notification is required, how timely it needs to be, and what information leads to identity theft.

Setting a national standard benefits consumers by ensuring that every business must look at their activities and make sure they are taking reasonable security measures. A national standard allows businesses to focus on securing information and systems instead of trying to figure out how to comply with a host of different State laws with teams of lawyers. Consumers benefit from consistency in security and breach notification no matter what State they live in.

We are particularly concerned with the impact these criminal acts have on consumer confidence, economic growth, and job creation. The criminals are in this for the money, so we need to make it far harder to steal an identity or use stolen information to make purchases. The cost to consumers is well into the billions of dollars. No committee is more aware than this one about how central the online economy is to our future. A data breach bill is the first step to securing that future.

Mr. UPTON. I yield the balance of my time to the vice chair of the full committee, Marsha Blackburn.

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I want to thank the chairman of the subcommittee for calling the hearing, and I want to welcome all of our witnesses today. We are indeed looking forward to hearing what you have to say.

As has been referenced by Mr. Welch, we have spent a couple of years working on the issues of privacy and data security. We have done this in a working group or a task force and drilling down, making certain that we have a good understanding of defining the problem and then looking at the opportunities for addressing that. So we come to you from that basis of work. And Ms. Schakowsky, Mr. Olson, both served on this task force with us.

Last October Director Comey from the FBI said there are two kinds of big companies in the United States: those that know they have been hacked by the Chinese and those that don't know they have been hacked by the Chinese. That is pretty apropos, and we know that it applies to all sizes of companies, as Chairman Upton just said.

Because of that, we understand that there are a few things that we need to look at: preemption and making certain that we have the standard, that this is easily communicated, that our constituents and the citizens understand what is the toolbox that they have for protecting, as I define it, the virtual you, whether that virtual you is they themselves individually, they themselves the small business person, or the corporate entity that is looking to protect its product and its name.

Now, I come from Nashville. We have a lot of entertainment, healthcare, and financial services that are watching this issue closely. They want to make certain that we get this right the first time.

With that, I yield back the balance of my time.

Mr. BURGESS. The gentlelady yields back. The Chair now recognizes the ranking member of the full committee, 5 minutes for an opening statement, Mr. Pallone from New Jersey.

**OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY**

Mr. PALLONE. Thank you, Mr. Chairman. I first wanted to congratulate Dr. Burgess on his appointment as the chairman. I will say, though, that having spent last evening with you on rules, I am not going to congratulate you on continuing on rules because I don't know what possible reason you could have for continuing to stay there. But everyone makes their own decisions around here.

I do look forward to working with you on many issues, starting with the issue of today's hearing, data security and breach notification. I also wanted to thank Ms. Schakowsky for her continued service as the Democratic Ranking Member.

The title of this hearing, What are the Elements of Sound Data Breach Legislation?, assumes that legislation is needed, and I agree that it is time to legislate but only if the result is a strong bill that puts consumers in a better place than they are today. Right now millions of consumers are being hit with endless waves of breaches. Criminal hackers will always target our communities, and while we cannot expect to eliminate data breaches, we can work harder to reduce the number of breaches and better protect consumers' information. Just as we expect a bank to lock its vaults of money, we should expect that companies lock and secure personal consumer information. Unfortunately, that is not happening. According to the Online Trust Alliance, over 90 percent of data breaches in the first half of 2014 could have been prevented had businesses implemented security best practices. Firms must do a better job of protecting information they demand of consumers, and preventing breaches is not just best for the consumer, in the long run it is cheaper for companies as well.

And I believe that we should also expect companies to notify consumers in the event of a breach. During this hearing we will hear the often-repeated statistic that 47 States plus Washington, DC, Guam, Puerto Rico, and the Virgin Islands already have data breach notification laws on the books. While no one on either side of the aisle wants to unnecessarily burden businesses with duplicative or overlapping requirements, these State laws provide baseline breach notification to most Americans. In addition, businesses that operate nationally often follow the strictest State laws, giving our constituents strong data security and breach notification protections coverage regardless of what is written in any individual State law. And therefore, I can't support any proposal that supersedes strong State protections and replaces them with one weak Federal standard.

So Mr. Chairman, this subcommittee has had a tradition of being bipartisan, particularly on the issue of data security, and the 111th Congress' committee passed a compromise bill on the House Floor as H.R. 2221, and that bill was shepherded by then-Subcommittee Chairman Bobby Rush and was based on a bill crafted by former Subcommittee Chairman Cliff Stearns, and Chairman Upton, Vice Chairwoman Blackburn, and Chairman Barton were original cosponsors of these various bills.

So I just want to say I look forward to working with the subcommittee on a bipartisan basis to craft similar legislation and legislation that requires companies to have reasonable security measures in place and to provide notification to consumers once a breach has occurred.

[The prepared statement of Mr. Pallone follows:]

#### PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

I want to start by congratulating Dr. Burgess on his appointment as chairman. I look forward to working with him on many issues, starting with the issue of today's hearing, data security and breach notification. I also want to thank Ms. Schakowsky for her service as the Democratic ranking member.

The title of this hearing, "What are the Elements of Sound Data Breach Legislation?," assumes that legislation is needed. I agree that it is time to legislate—but only if the result is a strong bill that puts consumers in a better place than they are today.

Right now, millions of consumers are being hit with endless waves of breaches. Criminal hackers will always target our communities. And while we cannot expect to eliminate data breaches, we can work harder to reduce the number of breaches and better protect consumers' information. Just as we expect a bank to lock its vaults of money, we should expect that companies lock and secure personal consumer information.

Unfortunately, that is not happening. According to the Online Trust Alliance, over 90 percent of data breaches in the first half of 2014 could have been prevented had businesses implemented security best practices. Firms must do a better job at protecting the information they demand of consumers. Preventing breaches is not just best for the consumer, in the long-run, it is cheaper for companies as well.

I believe that we should also expect companies to notify consumers in the event of a breach. During this hearing, we will hear the often repeated statistic that 47 States, plus Washington, DC, Guam, Puerto Rico, and the Virgin Islands, already have data breach notification laws on the books. While no one, on either side of the aisle, wants to unnecessarily burden business with duplicative or overlapping requirements, these State laws provide baseline breach notification to most Americans. In addition, businesses that operate nationally often follow the strictest State laws, giving our constituents strong data security and breach notification protections coverage regardless of what is written in any individual State law. Therefore, I cannot support any proposal that supersedes strong State protections and replaces them with one weak Federal standard.

Mr. Chairman, this subcommittee has had a tradition of being bipartisan, particularly on the issue of data security. In the 111th Congress, this committee passed a compromise bill on the House floor as H.R. 2221. That bill was shepherded by then-Subcommittee Chairman Bobby Rush and was based on a bill crafted by former Subcommittee Chairman Cliff Stearns. Chairman Upton, Vice Chairman Blackburn, and Chairman Emeritus Barton were original cosponsors of these various iterations.

I look forward to working with this subcommittee on a bipartisan basis to craft similar legislation—legislation that requires companies to have reasonable security measures in place and to provide notification to consumers once a breach has occurred.

Thank you.

Mr. PALLONE. I yield back, Mr. Chairman.

Mr. BURGESS. The gentleman yields back his time. The Chair would remind all members on the subcommittee that they are able to insert their written statements for the record.

And I do want to welcome our witnesses for being here this morning. I thank all of you for agreeing to testify before the committee. Our witness panel for today's hearing will include Ms. Elizabeth Hyman who is the Executive Vice President of Public Advocacy for TechAmerica, and she will be testifying on behalf of the Computing Technology Industry Association. We also have Ms. Jennifer Glasgow, the Global Privacy Officer for Acxiom Corporation; Mr. Brian Dodge, who is the Executive Vice President of Communications and Strategic Initiatives on behalf of the Retail Industry Leaders Association; and Mr. Woodrow Hartzog, an Associate Professor of Law at Samford University's Cumberland School of Law in Birmingham, Alabama.

Our first witness is Ms. Elizabeth Hyman, and you are recognized for 5 minutes.

**STATEMENTS OF ELIZABETH HYMAN, EXECUTIVE VICE PRESIDENT, PUBLIC POLICY, TECHAMERICA, COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION; BRIAN A. DODGE, EXECUTIVE VICE PRESIDENT, COMMUNICATIONS AND STRATEGIC INITIATIVES, RETAIL INDUSTRY LEADERS ASSOCIATION; JENNIFER BARRETT-GLASGOW, GLOBAL PRIVACY OFFICER, ACXIOM CORPORATION; AND WOODROW HARTZOG, ASSOCIATE PROFESSOR OF LAW, CUMBERLAND SCHOOL OF LAW, SAMFORD UNIVERSITY**

#### **STATEMENT OF ELIZABETH HYMAN**

Ms. HYMAN. Good morning, and thank you very much for having us, Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the Subcommittee on Commerce, Manufacturing, and Trade. We appreciate your convening this hearing and for giving us the opportunity to provide our insights on the important issue of consumer data breach notification.

My name as you mentioned is Elizabeth Hyman. I am the Executive Vice President of Public Advocacy for TechAmerica, the public policy department of The Computing Technology Industry Association, CompTIA. CompTIA is headquartered in Downers Grove, Illinois, and we represent over 2,200 technology companies, a large number of which are small- and medium-sized firms.

Technology companies take their obligations to protect consumers' information very seriously. Data is the life-blood of the Internet economy, and protecting consumers' information is not only a responsibility of the industry but also a crucial business practice. Failure to do so will lead to a loss in customer faith and damage to a business' reputation.

Unfortunately, as has been pointed out, criminals remain intent on stealing information. Data breaches are sadly all too common in 2015, and thus we need strong rules in place to inform consumers when a harmful breach occurs and to provide the necessary information to enable consumers to take the necessary steps to protect themselves.



As you are all well aware and has been stated, there currently is no Federal standard for data breach notification. Instead, 47 different States, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, all have their own separate data breach notification laws and requirements.

Furthermore, States are regularly changing and updating their data breach notification laws. This year we have already seen 17 bills introduced in seven States in just the first 2 weeks of State legislative sessions. With the increasingly mobile and decentralized nature of our economy, most companies are under the umbrella of multiple State laws at all times. This patchwork of State laws creates significant compliance costs with no additional protection for consumers since no two State data breach laws are exactly the same. In fact, many are in conflict with one another. A Federal data breach notification standard is thus necessary to protect consumers and ensure that companies can respond quickly and effectively after a breach.

Responding to a data breach for a company of any size is difficult, especially given the need to assess whether the breach could trigger notification provisions in any one of 47 States, whether they have any consumers that live in any of those States, who to notify, how to notify, what information to include, and what the timelines are for notification.

Small- and medium-sized businesses face particularly difficult compliance challenges. To address their obligations to resolve the breach, gather information, and notify the necessary parties, these companies often rely on cyber-insurance, payment processors, or outside counsel to help implement a response plan. None of these options is cheap.

Thus, the key to any Federal data breach notification law will be finding a single standard that maintains strong requirements but allows companies to focus on the important work of protecting their customers in the wake of a breach.

In crafting a Federal data breach standard, we would suggest a few key provisions that are further outlined in my statement for the record. For example, any Federal data breach notification law needs to be the standard for all companies to comply with. It cannot simply just become the 48th standard that State can add to. In order to avoid the risks associated with overnotification, a Federal standard should ensure that consumers only receive notification about a breach when their information has actually been accessed and only when that information is likely to be used in a harmful manner.

Adequate time should be provided for companies to conduct a risk assessment in order to best assess the scope and depth of the breach. A circumscribed set of sensitive, personally identifiable information must be the basis for determining whether any notification should occur. We should try to avoid mandating specific technologies while also exempting companies from notification requirements where data is rendered unusable. Companies should not be punished for the criminal acts of others, and private rights of action regarding data breach notification should be explicitly banned.

In closing, I would like to thank the subcommittee for working on the issue of data breach notification. Unfortunately, our patch-

work of State laws, while well-intentioned, has created a burdensome and complex compliance regime. A strong, single standard that applies throughout the country will ensure our consumers are safer and ensure our companies are well-informed about how to respond to the growing threat of data breaches.

Security and economic growth are not mutually exclusive, and I would respectfully request that the solutions you draft through this subcommittee address both through a national data breach notification standard. Thank you.

[The prepared statement of Ms. Hyman follows:]

Prepared Testimony and  
Statement for the Record of

Elizabeth Hyman

**Executive Vice President, Public Advocacy**

**TechAmerica**, the public sector and public policy department of CompTIA |  
CompTIA.org

Before the

U.S. House Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing, and Trade

Hearing on

What Are the Elements of Sound Data Breach Legislation?

Tuesday, January 27, 2015

2123 Rayburn House Office Building

**Summary**

Compared to the current patchwork of state data breach notification laws, a single federal data breach notification standard will better protect consumers and allow companies to respond quickly and effectively following a breach. The key to any federal DBN law will be finding a single standard that maintains the strong consumer protections currently required by the states, but that does not overburden or impose inappropriate penalties on companies who should be focusing on notification and investigation in the wake of a breach. A federal standard should:

- Contain strong preemption language
- Avoid over-notification of consumers through
  - Requiring a significant risk of harm before notification
  - Allowing for adequate time for a risk assessment
  - A narrow definition of PII
- Avoid mandating specific technologies
- Encourage good security practices
- Forbid a private right of action

**Introduction**

Good morning Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the Subcommittee on Commerce, Manufacturing, and Trade. Thank you for convening this hearing on the important issue of consumer data breach notification. TechAmerica appreciates the opportunity to provide our insights as the Subcommittee explores the effectiveness of current state data breach laws, and considers whether Congress should enact legislation establishing a national breach notification standard.

My name is Elizabeth Hyman, and I am the Executive Vice President of Public Advocacy for TechAmerica, the public sector and public policy department of The Computing Technology Industry Association (CompTIA). We represent over 2200 technology companies, a large number of which are small and medium-sized Information Technology companies, and are committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world.

We commend the Subcommittee for making consumer data breach notification a priority. This issue is a matter of great concern for both consumers and for our member companies that engage in global electronic commerce and provide much of the infrastructure to make e-commerce possible.

Technology companies take their obligations to protect consumers' information very seriously. Data is the life-blood of the Internet economy and protecting consumers' information is not only a responsibility of the industry, but also a crucial business practice. Failure to appropriately protect consumers' information will lead to a loss in customer faith and damage to a business' reputation.

Unfortunately, the reality of today's world is that criminals are constantly trying to hack into databases to steal valuable information, and despite the extensive efforts companies employ to stop such criminals, some are bound to succeed. Data breaches are sadly a part of doing business in 2015, and thus we need strong consumer protections in place to inform consumers when a harmful breach occurs, and provide the necessary information to enable consumers to take steps to protect themselves from those who may have already obtained their information.

The current state of data breach notification law, however, does not meet this goal. As you are all well aware, there currently is no federal standard for data breach notification. Instead, 47 different states (all except for Alabama, New Mexico and South Dakota), the District of Columbia, Puerto Rico, Guam and the Virgin Islands all have their own separate data breach notification laws and requirements.

With the increasingly mobile and decentralized nature of our economy and data storage and dissemination technologies, most companies are under the umbrella of multiple state laws at all times. This patchwork of state DBN laws creates significant

compliance costs since no two state data breach laws are exactly the same. Moreover, many of these state DBN laws are in conflict with each other. For example, laws may vary as to when a data breach notice is triggered, the timeline within which notice must be provided, and what must be contained in the actual notice. This complex and burdensome system is costly and inefficient, and is potentially harmful to the very consumers it seeks to protect. A federal DBN standard is thus necessary to protect consumers and ensure that companies can respond quickly and effectively after a breach.

Responding to a data breach for a company of any size is difficult. It requires a company to first ascertain if a breach has occurred, and if so, what type of data may have been compromised; whether the data contains personally identifiable information (PII); what the risk is for consumers, business partners and others; how was it compromised; has the hole been plugged; and what are next steps. Concurrently, they also have to determine if consumer data was accessed, whether the type of data that was accessed could trigger data breach notification provisions in any one of 47 states, and if so, whether they have any consumers that live in any of those states assuming they even have that information. If a company does determine that notification may be required in some states, they then need to figure out who to notify, how to notify, what information to include, and what the timelines for notification are.

Small and medium-sized businesses, which make up a large portion of our 2200 members, face particularly difficult compliance challenges. To address their obligations to resolve the breach, gather information, and notify the necessary parties, these companies often rely on cyber-insurance, help from law enforcement or payment processors, or outside counsel to help them put together and implement a data breach response plan; none of these options is cheap.

Thus, the key to any federal DBN law will be finding a single standard that maintains the strong consumer protections currently required by the states, but that does not overburden or impose inappropriate penalties on companies who should be focusing on notification and investigation in the wake of a breach.

### **Strong Preemption Language**

Any federal data breach notification law must preempt state laws and requirements. Without strong preemption language, the entire basis for enacting a federal DBN standard disappears.

In addition to the compliance challenges already discussed, states are regularly changing and updating their DBN laws, adding yet another layer of complexity in trying to keep up with the changes. Last year, 23 different state DBN bills were introduced across the country, and this year we've already seen 17 bills introduced in 7 states in the first two weeks of the state sessions.



A federal standard needs to be *the* standard for all companies to comply with; it cannot simply become a 48<sup>th</sup> standard that states can add their own requirements atop. Overlaying more regulations on top of the existing patchwork of laws adds to the problem and does not help our companies protect consumers.

We do, however, believe that state attorneys general should be able to enforce the federal standard, as more cops on the beat helps protect consumers. But any federal standard should clearly state that companies cannot be penalized on both the state and federal levels for the same violation.

#### **Avoid Over-notification of Consumers**

It is essential that consumers only receive notification about a breach when their information has actually been accessed, and even then only when that information is likely to be used in a harmful manner. As former FTC Chairman Deborah Majoris has noted, over-notification will cause "consumers [to] become numb if they are continuously notified of every breach." Additionally, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and "phishing" attacks when bad actors hear through the media about notifications. Over-notification increases these risks.

To minimize the risk of fraud and identity theft that could result from consumer confusion due to over-notification, a federal DBN standard should contain three things: 1) Any federal framework should require consumer breach notification only when there is a *significant risk* that harm has or is likely to occur; 2) adequate time

for risk assessment; and 3) a careful definition of personally identifiable information.

#### *Significant Risk of Harm*

Without establishing a meaningful threshold and relevant requirements for notification, there is a very real likelihood of unintended, negative consequences for consumers, business entities and public authorities. To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when sensitive personal information has been accessed in a manner that creates a significant risk of harm.

#### *Adequate Time for Risk Assessment*

When a breach is discovered, one of the first things that a company must do is to conduct a risk assessment to determine the type of data that has been accessed and the risk that potential fraudulent use of the data could entail. This risk assessment is a vital component to a company's data breach response, and, depending upon the seriousness of the breach, may take some time to complete. We therefore ask that a federal standard "starts the clock" on a notification requirement only after the risk assessment has been completed.

Short-changing the risk assessment is dangerous to the company and consumers. If a company does not have adequate time to complete a risk assessment, there is a chance that the company may not have time to adequately assess the scope of the breach or the damage caused by the breach.

If a company has inadequate time to conduct a risk assessment, it may report that credit card data or other PII may have been accessed, only to find out later that none of that data was actually accessed. This type of over-notification could lead consumers to cancel their credit cards, often at significant expense to credit unions and other credit card issuers, as well as possible inconvenience to consumers, even though it turns out that such a reaction was unnecessary.

Alternatively a company may initially inform consumers that PII was not accessed, only to find out later that it was. This could lull consumers into ignoring the later, and more important, notice, potentially subjecting themselves to risk as a result of the initial under-notification.

Instead, we believe that getting the notification right could be more beneficial to consumers than rushing to notify with potentially erroneous information.

#### *Definition of PII*

Central to an effective framework is a meaningful definition of “sensitive personally identifiable information” that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of “sensitive personally identifiable information” be the basis for determining whether any notification should occur. For example, such a definition should not include publicly available information.

#### **Avoid Mandating Specific Technologies and Encourage Good Practices**

As part of the inquiry into whether the “sensitive personally identifiable information” obtained could be harmful to consumers, TechAmerica urges the Committee to consider whether the information accessed has been rendered unusable. For example, a number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction, that would render any data that is breached unusable. In those instances, the requirement to notify consumers should be unnecessary. Further, the legislation should exempt companies from notification requirements where data is rendered unusable.

**No private rights of action**

Data breaches are criminal activity, as the President’s proposal to impose criminal penalties on entities that export data out of the U.S. implicitly acknowledges. Companies should not be punished for the criminal acts of others, and therefore any legislation in this space should explicitly ban private rights of action regarding data breaches and breach notification.

**Conclusion**

In closing, I would like to, again, thank the Subcommittee for working on the issue of data breach, which continues to put consumers at risk. Unfortunately, the patchwork of state laws, while well-intentioned, has created such a burdensome and complex compliance regime that it is now contributing to the problem; not helping to solve it. A strong, single standard that applies throughout the country will ensure

that consumers are safer and will help ensure that companies are aware of how to respond to the growing threat of data breaches.

Security and economic growth are not mutually exclusive and I would respectfully request that the solutions you draft through this Subcommittee address both through a national data breach notification standard.

Mr. BURGESS. The gentlelady yields back. The Chair would now recognize Mr. Brian Dodge, the Executive Vice President of the Retail Industry Leaders Association, 5 minutes for your testimony, sir. Thank you.

#### **STATEMENT OF BRIAN A. DODGE**

Mr. DODGE. Chairman Burgess, Ranking Member Schakowsky, and Members of the committee, my name is Brian Dodge, and I am an Executive Vice President with the Retail Industry Leaders Association. Thank you for the opportunity to testify today about data breach legislation and the steps that the retail industry is taking to address this important issue and to protect consumers.

RILA is the trade association of the world's largest and most innovative companies. Retailers embrace innovative technology to provide American consumers with unparalleled services and products. While technology presents great opportunity, nation-states, criminal organizations, and other bad actors also are using it to attack businesses, institutions, and governments. As we have seen, no organization is immune from attacks. Retailers understand that defense against cyberattacks must be an ongoing effort.

RILA is committed to working with Congress to give Government and retailers the tools necessary to thwart this unprecedented attack on the U.S. economy and bring the fight to cybercriminals around the world.

As leaders in the retail community, we are taking new and significant steps to enhance cybersecurity throughout the industry. To that end, last year RILA formed the Retail Cyber Intelligence Sharing Center in partnership with America's most recognized retailers. The Center has opened a steady flow of information between retailers, law enforcement and other relevant stakeholders.

In addition to the topics this hearing will cover today, one area of security that needs immediate attention is payment card technology. The woefully outdated magnetic stripe technology used on cards today is the chief vulnerability in the payments ecosystem. Retailers continue to press banks and card networks to provide U.S. consumers with the same chip and PIN technology that has proven to dramatically reduce fraud when it has been deployed elsewhere around the world.

Before I discuss what RILA believes the components of sound data breach legislation are, I will briefly highlight the significant data breach and data notification laws with which retailers currently comply. As has been said, 47 States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have adopted data breach notification laws. In addition to the 47-plus existing State data breach notice laws, retailers are subject to robust data security regulatory regimes as well. The Federal Trade Commission has settled at least 50 cases against businesses that it charged with failing to maintain reasonable data security practices. These actions have created a common law of consent decrees that signal the data security standards expected of businesses. Additionally, inadequate data security measures for personal information can lead to violations of expressed State data security laws. Also, many States has so-called little FTC acts that can be used to enforce

against what Attorneys General deem to be unreasonable data security practices.

Finally, retailers voluntarily and by contract follow a variety of security standards including those maintained by the payment card industry, NIST, and the International Organization of Standardization.

While retailers diligently comply with this range of data security notice and data requirements, a carefully crafted Federal data breach law can clear up regulatory confusion and better protect and notify consumers.

RILA supports a Federal data breach that is practical, proportional, and sets a single national standard. RILA urges the committee to consider data breach legislation that creates a single national notification standard that allows business to focus on quickly providing affected individuals with actionable information; that provides flexibility in the method and timing of notification; that ensures that notice is required only when there is a reasonable belief that the breach has or will result in identity theft, economic loss, or harm; that ensures that the responsibility to notify is that of the entity breached but provides the flexibility for entities to contractually determine the notifying party; that establishes a precise and targeted definition for personal information; that recognizes that retailers already have robust data security obligations and that security must be able to adapt over time.

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

We look forward to working with the committee on specific language to address each of these above goals. I thank the committee for considering the need for preemptive data breach legislation and look forward to answering your questions.

[The prepared statement of Mr. Dodge follows:]



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

**TESTIMONY OF**

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

**RETAIL INDUSTRY LEADERS ASSOCIATION**

**BEFORE THE**

**HOUSE ENERGY AND COMMERCE COMMITTEE  
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE**

**HEARING ON**

***"WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?"***

**JANUARY 27, 2015**

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

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

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



### Key Cybersecurity Issues for Retailers

As leaders in the retail community, we are taking new and significant steps to enhance cybersecurity throughout the industry. To that end, RILA formed the Retail Cyber Intelligence Sharing Center (R-CISC) in 2014 in partnership with America's most recognized retailers. The Center has opened a steady flow of information sharing between retailers, law enforcement and other relevant stakeholders. These efforts already have helped prevent data breaches, protected millions of American customers and saved millions of dollars. The R-CISC is open to all retailers regardless of their membership in RILA.

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

One area of security that needs immediate attention is payment card technology. RILA members have long supported the adoption of stronger debit and credit card security protections. The woefully outdated magnetic stripe technology used on cards today is the chief vulnerability in the payments ecosystem. This 1960s era technology allows cyber criminals to create counterfeit cards and commit fraud with ease. Retailers continue to press banks and card networks to provide US consumers with the same Chip and PIN technology that has proven to dramatically reduce fraud when it has been deployed elsewhere around the world. According to the Federal Reserve, PINs on debit cards make them 700 percent more secure than transactions authorized by signature.<sup>1</sup>

Increasing cyber threat information sharing also is vital to defeating sophisticated and coordinated cyber actors. RILA strongly supports cybersecurity information sharing legislation that provides liability protections for participating organizations. Legislation also should increase funding for government sponsored research into next generation security controls and enhance law enforcement capabilities to investigate and prosecute criminals internationally. The cyber-attacks faced by every sector of our economy constitute a grave national security threat that should be addressed from all angles.

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

---

<sup>1</sup> Federal Reserve, "2011 Interchange Fee Revenue, Covers Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions," (March 5, 2013).

receive timely and accurate information following a breach. To place in context the need for preemptive federal data breach legislation, we provide below a brief overview of the significant data security and breach notification laws with which retailers currently comply.

### **Existing Data Security and Breach Notification Laws**

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

In addition to 47 state data breach notice laws and the laws in DC and the US territories, retailers are subject to robust data security regulatory regimes relating to protections for sensitive personal information. At the federal level, the Federal Trade Commission (FTC) is the primary regulator of data security for most businesses across a wide array of industry sectors, including the retail sector. Under Section 5 of the FTC Act, the FTC has authority broadly to bring enforcement actions against companies that engage in "unfair or deceptive acts or practices in or affecting commerce."<sup>2</sup> Although the FTC has not promulgated data security rules, its robust enforcement activity has collectively created a "common law" of consent decrees that tend to signal what is expected from businesses regarding the collection, use, and protection of personal information. The consent decrees usually involve non-monetary remedies requiring the implementation of comprehensive company privacy or data security programs with biennial audits for up to 20 years. The FTC can impose penalties of up to \$16,000 per violation for violations of a consent decree.

The FTC uses both its authority to prevent consumer deception and unfairness to enforce data security standards.<sup>3</sup> Pursuant to its authority to prevent deceptive acts or practices, the FTC can and does bring enforcement actions against companies that have failed to comply with their data security representations and statements in their public-facing privacy policies or other disclosures. Pursuant to its authority to prevent unfair acts and practices, the FTC has pursued companies that have failed to deploy reasonable and appropriate security measures to protect the sensitive personal information they possess or handle (e.g., Social Security numbers, financial

<sup>2</sup> 15 U.S.C. § 45(a)(1).

<sup>3</sup> FTC, US Senate Banking Committee Hearing on Safeguarding Consumers' Financial Data (2014), available at [http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore\\_id=c6f6163c-ae31-4091-8e7c-c10e1eebbe84](http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=c6f6163c-ae31-4091-8e7c-c10e1eebbe84).

account or payment card information, and other information that can lead to fraud or identity theft) using its Section 5 enforcement power.

Since 2001, the FTC has settled at least fifty cases against businesses that it charged with failing to provide reasonable data security practices. The FTC conducts enforcement investigations with a focus on reasonableness, and has stated that “a company’s data practices must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.”<sup>4</sup> Over time, the FTC’s enforcement actions and other guidance materials,<sup>5</sup> have created a robust set of data security expectations applicable to businesses under its jurisdiction. The FTC expects that companies implement a comprehensive information security program containing safeguards to address administrative, physical and technical risks to personal information.

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

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

#### **RILA Supports Sound Data Breach Legislation**

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

<sup>4</sup> FTC, US Senate Banking Committee Hearing on Safeguarding Consumers’ Financial Data, 4 (2014), available at [http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore\\_id=e6f6163c-ae31-4091-8e7c-c10e1eebbe84](http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=e6f6163c-ae31-4091-8e7c-c10e1eebbe84).

<sup>5</sup> See FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>.

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

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

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

The fifth goal of data breach legislation should be to avoid an overly broad scope. Retailers support a precise and targeted definition of personal information. It is important that notice and data protection occurs only when consumers face real peril from the exposure of sensitive data and need to be vigilant and potentially take action. An overly broad definition that includes harmless or publicly available data will both detract from the effectiveness of the notice (over-notifying) and chill the innovative use of data by the private sector. Differentiating between truly sensitive data requiring more restrictive security controls and harmless data that can be used more dynamically to create the next great product, service, or customer experience is vital to retailer innovation. Sweeping harmless data into the personal information definition undermines product development and the future economic growth of 21<sup>st</sup> century retailers. Also, an overbroad definition of personal information undermines a core goal of breach notice legislation, which is to provide carefully calibrated notice allowing consumers to prevent harm. Consumers that begin to ignore important communications are powerless to mitigate harm.

The sixth goal of data breach legislation should be to protect consumer data. Retailers support a carefully calibrated reasonable data security standard. If policymakers choose to address data security, the law must be carefully calibrated to recognize existing obligations and encourage companies to adhere to leading security practices. Legislating technology and prescribing technical standards will undermine cybersecurity innovation. The rapid pace of technological

change ensures the obsolescence of laws that are not technology neutral. Specific standards are best left to multi-stakeholder open standards setting organizations with the technical expertise, agility, and ability to move at Internet speed.

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

We look forward to working with the Committee on specific language to address each of the above goals.

**Retailers are Committed to Protecting Customer Data and Enhancing Consumer Trust**

Retailers are committed to protecting our customers through investments in cybersecurity technology and personnel, increased cyber threat information sharing through a new law and the Retail Cyber Intelligence Center, and support for sound federal data breach legislation that is practical, proportional and sets a single national standard that replaces the patchwork of state laws in place today. We are engaging with policymakers and all stakeholders to advance each of these initiatives. I thank the Committee for considering the need for preemptive data breach legislation and look forward to answering your questions.

Mr. BURGESS. The gentleman yields back. The Chair would now like to recognize Jennifer Barrett-Glasgow, the Global Privacy Officer for Acxiom, headquartered in Little Rock, Arkansas. Thank you for your testimony today, 5 minutes.

#### **STATEMENT OF JENNIFER BARRETT-GLASGOW**

Ms. BARRETT-GLASGOW. Chairman Burgess, Ranking Member Schakowsky, members of the committee, thank you for holding this hearing today. I am Jennifer Barrett-Glasgow, Global Privacy Officer for Acxiom, headquartered in Little Rock, Arkansas. Acxiom has two lines of business. We offer primarily to large businesses, not-for-profit organizations, political parties, and candidates and Government agencies. First, we offer computer processing services for our clients' information which includes ensuring that information is accurate, analyzing the information to help our clients understand their customers better so they can improve their offerings, and our digital reach services which enable our clients to market to audiences across all digital channels. These services represent over 80 percent of our total business in the United States.

Second, we provide a line of information products to clients in three categories: fraud management, telephone directories, and marketing. And these products support all channels of communication, offline, online, mobile, and addressable television.

Acxiom supports enacting a data security and breach notification bill, and I would like to mention some of the provisions that we think should and should not be included. Regarding data breach notification provisions, first, the bill needs to include strong preemption for State laws. As stated earlier, 47 States and 4 territories have breach laws, and every year a number of these change. Businesses and consumers will benefit from having one recognizable standard.

Second, there should be a harm-based trigger for notification. Consumers shouldn't get meaningless notices when there is no risk of harm. Businesses will have to evaluate whether there is a reasonable risk if there are penalties for failing to notify, and we will do that responsibly without Congress needing to spell out how it should be done.

Third, legislation should also provide a reasonable timeframe for notification. Consumers do need to be notified promptly, but it is critical to understand the extent and means of the breach and to give law enforcement time to identify and hopefully even apprehend the bad guys. Fixed statutory deadlines do not accomplish these objectives.

Fourth, penalty provisions should be reasonable, and we do not believe there should be a private right of action. Companies who take reasonable precautions but who still get breached are victims, too. Regarding data security language, just as with breach notification, having a single data security standard is more efficient for companies than multiple State standards. This is more important for some businesses and other entities than it is for Acxiom. We process data for other companies, and our security is assessed by clients upwards of 80 times a year, plus we conduct our own audit internally. So we already meet multiple client standards in addition to those set by law.

Next, because the bad guys' capabilities keep changing, legal and regulatory data security standards need to be extremely flexible to allow adaptive compliance to keep ahead of the threats.

And last, Acxiom believes that businesses have a responsibility to educate their employees about security risks and that Government has a role to play in educating the general public on these topics.

Where once the purpose of passing a data security law might have been to ensure companies were thinking enough about security, today we believe Congress should think about security breach legislation more like it has thought about cybersecurity legislation. How can the industry and Government and law enforcement work together to keep ahead of these threats.

Finally, a comment on what should not be included in this legislation. Congress should keep this bill focused on data security and breach notification. There is bipartisan support for enacting a good bill into law on these issues. In the past, other issues have crept into data breach bills, and this has hurt the chances of enactment. For example, some previous bills have included provisions for data brokers, and while Acxiom would be considered a data broker under any definition, it already offers the kinds of provisions seen in past bills through our web portal, [AboutTheData.com](http://AboutTheData.com). The problem has been the definition of data brokers. It was quite broad and included many companies that don't consider themselves to be one. This has stymied enactment of these bills. We urge you to keep the bill clean so we can finally put a good consensus Federal data security and breach notification law into place.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Ms. Barrett-Glasgow follows:]

**WRITTEN TESTIMONY OF**



**JENNIFER BARRETT-GLASGOW  
GLOBAL PRIVACY OFFICER  
ACXIOM CORPORATION**

**BEFORE THE  
UNITED STATES HOUSE  
COMMITTEE ON ENERGY AND COMMERCE  
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE**

**HEARING ON "WHAT ARE THE ELEMENTS OF  
SOUND DATA BREACH LEGISLATION?"**

**JANUARY 27, 2015**



Chairman Burgess, Ranking Member Schakowsky, distinguished Members of the Committee, thank you for holding this hearing and taking the time to address much needed federal legislation with regards to data security and data breach notification. I am very pleased to be here today, and Acxiom appreciates the opportunity to participate in this hearing and the overall discussion surrounding these issues.

Acxiom's business consists of large scale computer processing services, including more recently specialized services to enable our clients to reach their marketing audiences via mobile, television and online, which we refer to as our "digital reach service", and several information products. We help our clients successfully manage audiences they wish to reach, connect with these audiences, personalize experiences with their customers and create profitable customer relationships by sourcing and analyzing the data they collect.

Acxiom understands that we have an inherent responsibility to safeguard the personal information we process for our clients and the information we bring to the market. Therefore, we work within our industry and across the commercial spectrum, as well as with federal, state, and international governments to develop and implement best practices for the collection, use, and protection of data. We have been recognized for our efforts to meet and exceed the guidelines of the Digital Advertising Alliance, Interactive Advertising Bureau, Mobile Marketing Association and Direct Marketing Association, among others. We limit the use of our data depending on the type of data it is and the permissions associated with that data. And, we are proud to be the first and only information services company to offer consumers online access to and control of marketing data, which we do through a web portal, [www.AboutTheData.com](http://www.AboutTheData.com).

#### **About Acxiom Corporation**

Acxiom was founded in 1969 in Little Rock, Arkansas. We are headquartered there, with operations throughout the United States, including in California, Illinois, New York, Ohio, Tennessee, and Texas. The company also has offices in eight countries across Europe and Asia. From a small startup company in Arkansas, Acxiom Corporation has grown into a publicly traded corporation with some 5,500 employees worldwide.

Acxiom's U.S. business includes two distinct components: our large scale computer processing services, which includes our digital reach service, and a line of information products. Acxiom's computer services represent over 80% of the company's business and include a wide array of leading technologies and specialized computer services focused on helping clients manage their own customer information. These services would include things such as ensuring accurate name, address, and contact information; and analytics to help companies gain insights into their customers so they can improve their offerings. Our digital reach service enables our clients to reach marketing audiences across all digital channels. These services are offered primarily to large businesses, not-for-profit organizations, political parties and candidates, and government agencies. Acxiom's private sector computer services clients represent a "who's who" of America's leading companies and include 49 of the Fortune 100. Acxiom helps these clients improve the loyalty of their customers and increase their market share, while reducing risk and assisting them with their compliance responsibilities under state and federal law. Finally, Acxiom helps government agencies improve the accuracy of the personal information they hold.

The balance of Acxiom's business comes from information products. Our information products are comprised of three categories: fraud management products, telephone directory products, and marketing products. These products each play a unique role, helping to fill an important gap in today's business-to-consumer relationship and support three channels: online, mobile and addressable television. Our information products represent less than 20 percent of the company's total business.

Acxiom's fraud management products are sold to companies and government. These verification services validate that a person is who he or she claims to be.

Acxiom's telephone directory products include name, address and published telephone information. This information is compiled from the white and yellow pages of published U.S. and Canadian telephone directories and from information available from the various directory assistance services provided by the telephone companies. This information enables businesses and consumers to locate other businesses or consumers and powers many of the web white and yellow page services.

Acxiom's marketing information products provide demographic, lifestyle and interest information to companies to reach prospective new customers who are most likely to have an interest in their products and to better understand and serve the needs of existing customers. They are compiled from publicly available data, from public records, from surveys and from summarized customer information where appropriate notice and choices has been provided.

To understand the critical role Acxiom plays in facilitating the nation's economy and safeguarding consumers, it is also important to understand what the company does not do. Acxiom does not maintain one big database that contains detailed information about all individuals. Instead, the company develops discrete databases tailored to meet the specific needs of Acxiom's clients - entities that are appropriately screened and with whom Acxiom has legally enforceable contractual commitments. Acxiom does not provide information on individuals to the public, with the exception of our telephone directory product.

#### **Our Commitment to the Ethical Use of Data**

At Acxiom, we take data security very seriously. We have a longstanding tradition and engrained culture of protecting and respecting consumer interests in our business. We recognize that we have a responsibility to safeguard the personal information we hold and process on behalf of our clients and that we collect for our information products. To that end, the company is today, and always has been, a leader in developing self-regulatory guidelines and in establishing security and privacy policies and practices. For the 46 years we have been in business handling data, Acxiom has focused on assuring a safe environment for the information. We have in place a Security Oversight Committee that is headed by a Chief Security Officer with more than 30 years of IT experience, and we were the first company in the world to have a Global Privacy Executive – the position I have held since its inception in 1991.

Our security program is designed to exceed federal requirements for safeguarding data. We are often a leader in adopting new security techniques and protocols for the protection of data. As an example, even though Acxiom's marketing information products are not covered by the Gramm-Leach-Bliley Act (GLBA), we nevertheless apply GLBA Safeguard Rule to those products. Ultimately, Acxiom's approach to information security goes beyond what is required by either law or self-regulation.

Our commitment to security also comes from our first hand experience with data breaches. In 2003, the passwords on a server that resided outside our main system firewalls were hacked and many of the lists transferred by the server stolen. Acxiom used this server to transfer marketing lists between Acxiom and our clients. While marketing lists usually do not contain sensitive data, our standard protocol was to encrypt any sensitive data on these files, so no consumer was harmed by the incident. We were also fortunate that the collective efforts of Acxiom and law enforcement resulted in apprehending and bringing to justice the criminals involved in this breach. Furthermore, we learned a lot about both the risks that companies face as well as how to effectively work with the authorities when such incidents occur.

We have long been a leader in data stewardship, consumer education and transparency. Acxiom believes in giving consumers a voice and a choice. And while we've long offered consumer access and correction to our Fraud and Risk data products, we recognized the need to become even more transparent with our marketing information products. In 2013 we launched the first-of-its-kind marketing data access portal, [www.AboutTheData.com](http://www.AboutTheData.com). This is a website where consumers can log in and see what information Acxiom has gathered about them that is used for marketing purposes. Once there, consumers can update, modify and delete the information, and of course opt out from Acxiom's marketing data products altogether. This site also hosts information that educates consumers on how marketing data is used and why this use might be of value to them. This type of consumer voice and choice over marketing data, we believe, should be the industry standard. To date, about 750,000 people have visited the portal, approximately 16% have edited one or more data elements about themselves and less than 3 percent of visitors have opted-out. Acxiom was the first to offer this type of transparency, and we remain the only marketing services company to do so at present.

We have not stopped there. More recently Acxiom has partnered with the Better Business Bureau to help launch their Digital IQ initiative to broaden consumer's knowledge on the use of data and help consumers develop skills for effectively navigating the digital world. Many consumers do not have a good understanding of how data is collected and used. We feel a responsibility – and believe it is a good business practice – to help them understand. We have also recently announced our own initiative, AcxiomData4Good. This initiative makes data accessible and actionable for charitable organizations to better deliver value and service to consumers and the community at large. This program leverages Acxiom's leadership in marketing data and analytics, along with our technology assets and talent, to improve and hopefully solve pressing community issues in the areas of health, education and humanitarian aid.

Finally, we have recently awarded a grant to fund the efforts of the Information Accountability Foundation to develop an operational Unified Ethical Framework that business and other organization can use to apply ethical governance to the use of marketing data.

#### **Axiom Supports Effective Federal Legislation**

The recent data breaches of large companies have once again highlighted the importance of data security and breach notification legislation. Axiom testified before this Committee almost 10 years ago advocating for federal legislation on data security and breach notification. Since then, the frequency and severity of breaches has increased substantially.

This Committee has invested significant time and energy over the past 10 years debating and passing multiple breach notice bills, but unfortunately Congress has been unable to enact any such legislation into law. In the interim, almost every state has enacted its own breach notice law, resulting in a web of varying and even conflicting requirements that are subject to frequent change by state legislatures.

This complex array of laws and regulations continues to fuel Axiom's strong support for preemptive federal legislation, providing both a ceiling and a floor, which benefits both businesses and consumers. Businesses would gain the benefit of more easily managed and understood compliance obligations, as well as increased regulatory certainty. There have been many formulations of preemption language over the years. One we would commend to the Committee is the following:

*No law, rule, regulation, requirement, standard or other provision having the force and effect of law relating to data security or notification following a breach of data security may be imposed under State law or the law of a political subdivision of a State on a person subject to this Act.*

From the consumer's perspective, a single federal standard not only increases their confidence in the safeguards protecting information businesses hold, but also makes notice procedures in the event of a breach clearer. It has been discussed many times before this Committee, but there is indeed a danger of over-notification – that consumers will not pay attention to a notice that matters because they have previously received notices under circumstances where they were not at risk. Therefore, Axiom supports a harm-based trigger for notification.

We also support a reasonable timeframe for the notice, such as one that requires notice “without undue delay.” An unduly short or specific statutory deadline may not provide enough time for companies and law enforcement to sufficiently investigate a breach in a manner that allows them to identify the means and extent of the breach, and gives law enforcement sufficient time to identify the perpetrators. Axiom also supports the type of extension mechanism the Energy & Commerce Committee has included in many breach notice bills over the years. If a law enforcement agency determines that notification would impede an investigation, notice can be delayed. The Administration's recent data breach notification proposal limits this delay to instances where it is requested by a federal agency; the Energy and Commerce Committee's broader language from previous bills is better.

We would like to highlight one other distinction between what the Energy & Commerce Committee historically has supported in data breach notice legislation and the President's proposal. The President's proposal includes an exemption from notice if a risk assessment shows there is "no reasonable risk" that the breach will result in "harm." The breached entity is required to conduct a risk assessment to determine absence of a reasonable risk of harm. Failure to conduct the risk assessment reasonably, or in accordance with generally accepted standards, is itself a separate violation of law. By contrast, previous Energy & Commerce bills do not create an additional possibility of violation of law. For notice to be determined to be unnecessary, the breached entity would need to determine that there is no reasonable risk of "identity theft, fraud, or other unlawful conduct" – harms that are cognizable under law. Practically, this would necessitate a risk assessment. However, this approach does not make an improper risk assessment – which could be inadvertent – a separate violation of law. Among the specific Energy & Commerce bills to which we are referring on this provision is H.R. 2221 from the 111<sup>th</sup> Congress, sponsored by the former Chairman of this subcommittee Mr. Rush and passed with bipartisan support. More recently this type of approach has been in Vice Chairman Blackburn's legislation.

Axiom also supports effective security measures. Axiom believes it is likely to meet any reasonable security requirement. As part of our clients' due diligence processes, our security is assessed and audited upwards of 80 times per year. This is in addition to our own internal audits. Through this collaborative process we have significantly grown our technical knowledge and expanded our security measures. However, perfect security simply does not exist. As the President noted in announcing his recent proposal, "[E]ven as we get better, the hackers are going to get better, too." Given the need to constantly adapt security tactics, we recognize that security requirements should not be legislated with too much specificity. Therefore, we advocate for flexible measures that set a flexible baseline for security such as applying the Gramm-Leach-Bliley Act Safeguards Rule to everyone.

Axiom believes that businesses have a responsibility to educate their employees about security risks and that government has a role to play in educating the public in general on these topics. Over the years, we have seen the intended use of information taken in a data breach expand from credit card and identity theft to very sophisticated scams based on the personal data that is stolen. We can collectively protect the American public better if individuals are more aware of these kinds of crimes and can be more vigilant about recognizing when they may be the target of such scams.

Our constant goal is to live up to the responsibility we have to safeguard personal information. In addition to state and federal laws, we are subject to industry guidelines and compliance directing that transparency is provided to consumers when the data was collected. Federal preemptive data security and breach notification legislation such as we recommend would bring greater regulatory certainty to Axiom and other businesses. Most important, such legislation would give greater confidence to consumers about the safety of their personal data.

It is Axiom's understanding that the Committee intends to keep this bill focused on breach notice and data security. We believe that is the right decision. Over the years, the enactment

prospects of data breach notification and security bills have been hampered by the inclusion of “privacy” provisions for which there is less consensus. In particular, various bills have included so-called “data broker” provisions, such as requirements that data brokers allow consumers to access and correct information about them, or to opt-out of use of information about them for marketing purposes. As I have mentioned, Acxiom already does and will continue to do these things. However, the bills invariably have pulled in hundreds, perhaps thousands of companies who do not consider themselves to be “data brokers,” which has generated opposition to bills that largely have had consensus support for the remainder of their provisions – at least the thrust of those provisions, if not the precise legislative language. There are plenty of important issues to debate regarding data, but we believe Congress will best serve the public by maintaining this bill as a breach notice and security bill, and addressing other issues separately to see if a consensus can develop around them.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing today and to assist Congress in identifying how to best safeguard the nation’s information. Acxiom is available to provide any additional information the Committee may request.

Mr. BURGESS. Thank you. The witness yields back. The Chair now recognizes Mr. Hartzog, 5 minutes for your testimony. Thank you, sir, for being here.

#### STATEMENT OF WOODROW HARTZOG

Mr. HARTZOG. Thank you. Chairman Burgess, Ranking Member Schakowsky, and members of the committee, thank you very much for inviting me to appear before you and provide testimony. My name is Woodrow Hartzog, and I am an associate professor of law at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School. I have spent the last 3 years researching the law and policy of data protection, data security, and responses to data breaches. My comments today will address what I have learned from this research.

In order to be sound, data breach legislation must further three fundamental goals: transparency, data protection, and remedies for affected individuals. The patchwork of existing State and Federal sector-specific laws further these goals, but aggressively preemptive Federal legislation risks counteracting these goals and weakening our critical data protection infrastructure. Hard-won consumer protections could be lost. In short, any data breach legislation that fails to advance these three goals will be counter-productive.

I would like to make two main points regarding the elements of sound data breach legislation. First, sound data breach legislation should be minimally preemptive of existing State- and sector-specific data breach laws. Data breach laws are relatively new. It is not yet clear what the most effective approach to data protection and data response is or should be. We need multiple regulatory bodies to ensure the adequate resources and experimentation necessary to respond to constantly evolving threats and new vulnerabilities. Additionally, preemption threatens to water down important existing robust data breach protections. There is a real risk that preemptive Federal legislation would do more harm than good. For example, Federal data breach legislation would reduce the level of protection many or most Americans currently have if it narrowed existing definitions of personal information, if it mandated a showing of harm before companies were required to send notification, or if it failed to require a notice to a centralized organization, like the office of the State Attorney General.

Data breach legislation would also be counter-productive if it created gaps in protection. Federal data breach legislation that preempts all State data breach laws could fail to cover data breaches that only affect the residents of one State. Additionally, preemptive legislation that only covered digitized records would fail to cover breaches involving paper records which remain a significant target for data thieves.

The second point I would like to make is that sound data breach legislation must also incorporate requirements for data security. While data breach notification is important, we must be sure not to ask too much of it. Under a pure data breach notification scheme, providing reasonable data security would be voluntary. The law should require not just encourage that companies reason-

ably secure their personal data. If people cannot trust that the entities that collect and store our personal information, the commerce, innovation, public health, our personal relationships, and our culture will all suffer. Ensuring that companies must provide reasonable data security will ensure that fewer breach notifications need to be sent at all.

One important way to fortify data security would be to give the Federal Trade Commission rule-making authority. Specific authority for data security would help the FTC further clarify data security standards, require data security from nonprofit entities such as educational institutions, and issue civil penalties.

Federal legislation should also preserve the regulation of data security by States and sector-specific agencies. The numerous Federal agencies that require data security are not redundant. Rather, they can and do coexist with unique expertise and regulatory authority. Even agencies with overlapping jurisdiction contribute valuable resources and have relatively harmonized approaches to data security.

Finally, data breach legislation must preserve the ability of States to regulate data security. Data security is both a national and a local issue sometimes affecting small but significant groups of State residents. Even in the case of large national breaches, residents of some States are hit harder than others. States are nimble and capable of continued experimentation regarding the best approach to regulating data security. They are also closer to those whose data was compromised and provide additional resources to alleviate the strain and cost to enforcement on Federal agencies.

The modern threat to personal data is still relatively new. The concept of data breach legislation is newer still. It is too early to start rolling back protections and consolidating agencies to cut costs. Instead, sound data breach legislation should reinforce the current trajectory of data breach law which involves multiple approaches and constantly evolving robust consumer protection. Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Hartzog follows:]



**PREPARED TESTIMONY AND STATEMENT FOR THE RECORD  
OF**

**WOODROW HARTZOG  
ASSOCIATE PROFESSOR OF LAW  
SAMFORD UNIVERSITY'S CUMBERLAND SCHOOL OF LAW**

**HEARING ON**

**“WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?”**

**BEFORE THE**

**SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE  
U.S. HOUSE OF REPRESENTATIVES**

**January 27, 2015  
2123 Rayburn House Office Building  
Washington, DC**

## I. INTRODUCTION

Chairman Burgess, Vice Chairman Lance, Ranking Member Schakowsky, and Members of the Committee, thank you for inviting me to appear before you and provide testimony. My name is Woodrow Hartzog and I am an associate professor of law at Samford University’s Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School. I write extensively about information privacy law issues and have published well over a dozen law review articles and other scholarly works. Most relevant to this hearing, I have spent the past three years researching the law and policy of data protection, data security, and responses to data breaches.<sup>1</sup> My comments today will address what I’ve learned from this research.

Instead of debating the finer points of any specific proposal for data breach legislation, I will focus my remarks on how the fundamental goals of data protection should guide any federal response to data breaches. These comments are made in my personal, academic capacity. I am not serving as an advocate for any particular organization. My remarks will focus on two points.

First, I will argue that sound data breach legislation should be minimally preemptive of existing state and sector-specific data breach laws. It is not yet clear what the most effective approach to data protection and breach response is. Multiple regulatory bodies are still needed to protect our personal information in order to ensure the adequate resources and experimentation necessary to respond to constantly evolving threats and new revelations about our vulnerability. Additionally, preemption threatens to water down some of the important existing robust data breach protections. There is a real risk that preemptive federal legislation would do more harm than good. Our critical data protection infrastructure will be weakened if federal legislation scales back protection, consolidates regulatory authority, and sets specific rules in stone. Data breach law must offer robust protection and be able to evolve quickly.

Second, I will argue that sound data breach legislation must also incorporate requirements for data security. While data breach notification is important, we must be sure we do not ask too much of it. The law should require, not just encourage, reasonable data security practices from companies that collect, process, and share personal information. This will fortify the protection of personal information in the United States and help ensure that fewer breach notifications need to be sent at all.

---

<sup>1</sup> See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014), available at <http://ssrn.com/abstract=2312913>; Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015), available at <http://ssrn.com/abstract=2461096>; Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIVACY & SECURITY LAW REPORT 577 (2014), available at <http://ssrn.com/abstract=2424998>; Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator: FTC v. Wyndham and its Implications*, 13 BNA PRIVACY & SECURITY LAW REPORT 621 (2014), <http://docs.law.gwu.edu/facweb/dsolove/files/BNA%20FTC%20v%20Wyndham%20FINAL.pdf>.

## II. THE GOALS OF DATA BREACH LEGISLATION

Data breach laws are relatively new. In the early 2000s it became clear that personal data was a critical component of our national infrastructure and that the threat to this data was mounting. The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4400 data breaches made public with a total of over 932 million records breached.<sup>2</sup> Unfortunately, data protection is a process largely hidden from consumers, who typically have no way of knowing if databases containing their personal information were compromised. It became clear that a legal response was necessary to ensure that companies were motivated to protect personal data and to keep users and the public informed about data breaches.

The first state data breach statute was passed by California in 2003.<sup>3</sup> Since that time, 47 states have adopted some form of data breach legislation. Additionally, federal legislation such as the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act also contain a notification requirement.<sup>4</sup> The main component of data breach legislation is to require companies to notify certain people and entities in the event of a breach. Many data breach laws often require companies to provide some measure of reasonable security for their data.

While the particular details of these laws vary, together they demonstrate a commitment to three clear goals. In order to be effective, data breach legislation must provide: 1) Transparency, 2) Data protection, and 3) Consumer remedies. The patchwork of existing state and federal sector-specific laws already further these goals. General federal legislation that preempts this protection and fails to ensure that these goals will continue to be realized will cripple our critical data protection infrastructure. Hard won consumer protections will be lost. In short, any data breach legislation that fails to advance these three goals will be counterproductive.

### A. Transparency

It is important to understand these values that animate data breach legislation in order to carefully craft law. Transparency is perhaps the most salient and important goal of data breach legislation. Transparency is primarily achieved through the notification function of these laws. While specific details vary, generally data breach notification laws require companies to notify affected individuals and, in some circumstances, media, the public, and centralized organizations, in the event of a data breach.<sup>5</sup> While public discussion

<sup>2</sup> PRIVACY RIGHTS CLEARINGHOUSE, *Chronology of Data Breaches: Security Breaches 2005 – Present*, <https://www.privacyrights.org/data-breach>.

<sup>3</sup> CAL. CIV. CODE §§ 1798.29, .82, .84 (2012).

<sup>4</sup> 16 C.F.R. § 682.3(a); 45 C.F.R. §§ 164.308–314; 16 C.F.R. §§ 314.3–314.4.

<sup>5</sup> *Id.*; ALASKA STAT. § 45.48.010 *et seq.* (2007); ARIZ. REV. STAT. § 44-7501 (2013); ARK. CODE § 4-110-101 *et seq.* (2004); CAL. CIV. CODE §§ 1798.29, .82, .84 (2012); COLO. REV. STAT. § 6-1-716 (2002); CONN. GEN. STAT. § 36a-701b (2011); DEL. CODE tit. 6, § 12B-101 *et seq.* (2011); FLA. STAT. §§ 501.171, 282.0041, 282.318(2)(i) (2010); GA. CODE §§ 10-1-910, -911, -912 § 46-5-214 (West); HAW. REV. STAT. § 487N-1 *et seq.* (2008); IDAHO STAT. §§ 28-51-104 to -107 (2008); 815 ILL. COMP. STAT. ANN. §§ 530/1 to 530/25 (2008); IND. CODE §§ 4-1-11 *et seq.*, 24-4.9 *et seq.* (2014); IOWA CODE §§ 715C.1, 715C.2 (2015);

about the efficacy of breach notification usually focuses on the individual whose data was compromised, there are actually four different constituencies that are served by the transparency goal of breach notification.

Of course, transparency primarily benefits individuals affected by a breach. When people are notified quickly of a breach, they know to look for evidence of fraud and identity theft. They can take remedial measures such as credit monitoring or even a credit freeze. If account credentials are compromised, notification prompts people to change their usernames and passwords on the compromised website as well as any other service where they use the same credentials.

Breach notification also benefits other companies that have personal data. News of data breaches travels quickly between chief security officers and others in charge of protecting the personal data controlled by a company. Companies that are in similar situations to those suffering a breach can learn how they might avoid the same fate. By learning the details of how information was compromised and what kinds of businesses and information is being targeted, other companies can proactively respond new threats.

Breach notification also advances the discipline and study of data security. By learning about new threats and tactics, industry experts and academics in the field of data security can improve the discipline of protecting data. Breach notifications can be aggregated to reveal important facts and trends that benefit an entire field, especially when laws require that notification be given to a centralized organization in addition to consumers. For example, the State Attorneys General in both California and New York have issued comprehensive reports that analyze the data obtained from breach notification laws.<sup>6</sup> These reports provide critical insights into the evolving threats to personal data.

---

KAN. STAT. § 50-7a01 *et seq.* (2008); KY. REV. STAT. ANN. §§ 365.732, 61.931 to 61.934 (West); LA. REV. STAT. §§ 51:3071 *et seq.* 40:1300.111 to .116 (West); ME. REV. STAT. tit. 10 § 1347 *et seq.* (2009); MD. CODE COM. LAW §§ 14-3501 *et seq.* (2013); MD. STATE GOVT. CODE §§ 10-1301 to -1308 (2007); MASS. GEN. LAW § 93H-1 *et seq.* (2006); MICH. COMP. LAW §§ 445.63, 445.72 (2014); MINN. STAT. §§ 325E.61, 325E.64 (2011); MISS. CODE § 75-24-29 (2014); MO. REV. STAT. § 407.1500 (2014); MONT. CODE §§ 2-6-504, 30-14-1701 *et seq.* (2014); NEB. REV. STAT. §§ 87-801, -802, -803, -804, -805, -806, -807 (2014); NEV. REV. STAT. §§ 603.A.010 *et seq.*, 242.183 (2013); N.H. REV. STAT. §§ 359-C:19, -C:20, -C:21 (2009); N.J. STAT. ANN. § 56:8-163 (2012); N.Y. GEN. BUS. LAW § 899-aa, N.Y. STATE TECH. LAW 208 (McKinney 2014); N.C. GEN. STAT. §§ 75-61, 75-65 (2012); N.D. CENT. CODE § 51-30-01 *et seq.* (2008); OHIO REV. CODE §§ 1347.12, 1349.19, 1349.191, 1349.192 (2004); OKLA. STAT. §§ 74-3113.1, 24-161 to -166 (2014); OR. REV. STAT. § 646A.600 to .628 (2011); 73 PA. STAT. § 2301 *et seq.* (2013); R.I. GEN. LAWS § 11-49.2-1 *et seq.* (West); S.C. CODE § 39-1-90 (West); TENN. CODE § 47-18-2107 (2014); TEX. BUS. & COM. CODE §§ 521.002, 521.053 (2014); TEX. ED. CODE § 37.007(b)(5) (2013); UTAH CODE §§ 13-44-101 *et seq.* (2010); VT. STAT. tit. 9 § 2430, 2435 (2007); VA. CODE § 18.2-186.6, § 32.1-127.1:05 (2012); WASH. REV. CODE § 19.255.010, 42.56.590 (2013); W.V. CODE §§ 46A-2A-101 *et seq.* (West); WIS. STAT. § 134.98 (2009); WYO. STAT. § 40-12-501 *et seq.* (2007); D.C. CODE § 28-3851 *et seq.* (2013); 9 GCA § 48-10 *et seq.*; 10 LAWS OF PUERTO RICO § 4051 *et seq.*; V.I. CODE tit. 14, § 2208.

<sup>6</sup> Kamala D. Harris, *California Data Breach Report* (October 2014), [https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data\\_breach\\_rpt.pdf](https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf); Eric T. Schneiderman, *Information Exposed: Historical Examination of Data Breaches in New York State* (2014), [http://www.ag.ny.gov/pdfs/data\\_breach\\_report071414.pdf](http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf).

Finally, breach notification raises the public awareness of threats to data and the importance of vigilance and data protection. When data breaches are made public due to notification laws, sometimes by laws mandating notice be given directly to media, the public becomes better informed of the importance of data protection. Ideally, this helps create a more cautious and sophisticated public that is less likely to be careless when sharing and protecting their personal data. Additionally, breach notifications can encourage productive communication between consumers and companies that collect personal information. When breaches are more on the minds of consumers they are more likely to enquire about and demand responsible data practices, either in negotiations or in the marketplace.

### **B. Data Protection**

Sound data breach legislation should also motivate companies to protect data. Pure notification statutes encourage companies to protect data by facilitating a reputational and financial penalty for those suffering a breach. Companies are not eager to have their data breaches made public. Not only does this news tend to tarnish a company's reputation in the eyes of current and potential consumers, but it also can negatively affect a company's reputation among its peers and potential partners or investors. Additionally, the cost of notification can be significant if the breach involves a large number of records. The reputational and financial cost of notification gives companies the incentive to protect data to minimize the likelihood of a breach. These costs also encourage companies to audit their data, assess risk, and develop a breach response plan ahead of time, all of which benefit those whose personal data is at risk.

Data breach legislation can also obligate companies to provide reasonable data security practices. Indeed, many state and sector-specific laws have data security requirements in addition to notification requirements.<sup>7</sup> As I argue below, mere incentives to secure data are not sufficient, given the critical importance of data protection in the modern world. Data breach legislation must require reasonable data security from companies.

### **C. Remedies for Individuals**

Finally, data breach legislation should provide remedies for individuals affected by a breach. The most common kind of remedy is some provision of services like credit monitoring or facilitation of a credit freeze. These services help an individual respond to identity theft and fraud. Data breach statutes differ as to the extent these services are to be offered or suggested.<sup>8</sup> These statutes also differ as to who the services and information are to be offered to. Some laws only provide remedies to those who have been actually

<sup>7</sup> See e.g. MASS. GEN. LAW § 93H-2 (West 2006); ARK. CODE ANN. § 4-110-104(b) (Supp. 2007); 2008 CONN. ACTS No. 08-167 (Reg. Sess.); NEV. REV. STAT. ANN. § 603A.210 (West Supp. 2007); N.C. GEN. STAT. § 75-64(a) (2007); OR. REV. STAT. ANN. § 646A.622(1) (West Supp. 2008); R.I. GEN. LAWS § 11-49.2-2(2) (Supp. 2007); UTAH CODE ANN. § 13-44-201(1)(a) (Supp. 2007); 45 C.F.R. §§ 164.308-.314.

<sup>8</sup> See e.g. CAL CIV. CODE § 1798.29 (West 2012) (requiring consumer notification including the time of breach and the toll free numbers and addresses of credit card reporting agencies in California); MD. STATE GOVT. CODE § 10-1305 (West 2007) (requiring consumer notice of the information breached, along with the contact information of the state Attorney General, the FTC and credit reporting agencies).

harm. Others provide some form of a remedy for all individuals affected by a breach. Additionally, the breach laws in 17 states provide for a private cause of action for individuals.<sup>9</sup> These protections help individuals recover from the loss of their personal information.

### III. THE IMPORTANCE OF MINIMAL PREEMPTION

Sound federal data breach legislation should only minimally preempt existing state and sector-specific data notification and security laws. Minimal preemption respects existing consumer protections and the ongoing uncertainty of how to best protect data in the information age. Existing federal data protection legislation has respected the multiple approaches to data protection. Legislation that weakens existing state and federal consumer protections by preempting them with weaker protections will jeopardize individuals. Legislation that frustrates the diversity of approaches and ability for laws to be modified will stunt the natural and important evolution of data protection policy.

#### A. State and Sector-Specific Protections Should Be Preserved

The current patchwork of state and sector-specific data breach laws covers a broad range of data and offers different forms of protection. Almost all of these laws advance the goals of transparency, protection, and remedies. There are three main ways by which aggressive federal preemption would be counterproductive.

First, federal legislation would leave people more vulnerable if it replaced robust substantive protections in state and sector-specific laws with weaker requirements. For example, if federal data protection legislation applied to fewer companies or kinds of personal information than existing law, mandated a showing of harm before companies were required to send notification, or failed to require notice to a centralized organization like the Office of the State Attorney General, it would reduce the level of protection many or most Americans currently have.

Second, data breach legislation would be counterproductive if it created gaps in protection. Federal data breach legislation that preempts all state data breach laws could fail to cover data breaches that only affect the residents of one state. Additionally, preemptive legislation that only covered digitized records would fail to cover breaches involving paper records, which remain a significant target for data thieves.

<sup>9</sup> ALASKA STAT. § 45.48.010 *et seq.* (West 2007); CAL CIV. CODE §§ 1798.29, .82, .84 (West 2012); DEL. CODE tit. 6, § 12B-101 *et seq.* (West 2011); LA. REV. STAT. §§ 51:3071 *et seq.* 40:1300.111 to .116 (West); MD. CODE COM. LAW §§ 14-3501 *et seq.* (West 2013); MD. STATE GOVT. CODE §§ 10-1301 to -1308 (West 2007); MASS. GEN. LAW § 93H-1 *et seq.* (West 2006); MINN. STAT. §§ 325E.61, 325E.64 (West 2011); N.H. REV. STAT. §§ 359-C:19, -C:20, -C:21 (2009); NEV. REV. STAT. §§ 603.A.010 *et seq.*, 242.183 (2013); N.C. GEN. STAT. §§ 75-61, 75-65 (West 2012); OR. REV. STAT. § 646A.600 to .628 (West 2011); R.I. GEN. LAWS § 11-49.2-1 *et seq.* (West); S.C. CODE § 39-1-90 (West); TENN. CODE § 47-18-2107 (2014); VT. STAT. tit. 9 § 2430, 2435 (West 2007); VT. STAT. tit. 9 § 2430, 2435 (West 2007); WASH. REV. CODE § 19.255.010, 42.56.590 (West 2013); D.C. CODE § 28-3851 *et seq.* (2013).

Finally, as I argue below, data breach legislation would be regressive and harmful if it consolidated total responsibility for data breach notification and security into one regulatory agency. Data protection is part of the critical infrastructure in the United States and requires multiple regulators who bring specific expertise and additional resources into the fold.

If federal legislation must be preemptive, it should only preempt state laws that address the same specific area as that federal law, for example, the notification response time. A better alternative would be for federal legislation to serve as a floor, not a ceiling for regulation. This would allow state and sector-specific laws to be more protective, but not less. Ideally, preemptive data breach legislation would strengthen data breach law by introducing new features not present in existing statutes and regulations.

#### **B. Data Breach Law Must Be Capable of Evolution and Continued Experimentation**

Data breach legislation should be minimally preemptive because multiple approaches are still needed to determine the best approach to data security and breach notification. While general principles can be agreed upon, more data is needed to determine the most effective particularized requirements of breach legislation. For example, the definition of personal information to be covered by the statute has been in flux since California passed the first data breach statute in 2003. Many breach laws contain a trigger requirement for notification that in some way is dependent upon a perceived risk of harm, which is a dubious and contested concept in policy and academic circles. The time frame for notice among statutes also varies between 5 to 30 days or is a more general standard such as "within the most expedient time possible and without unreasonable delay." A consensus has not even been reached on the optimal form and content of the notification itself.

Data breach law must remain nimble while such uncertainty persists. If the preemptive effect of federal data breach legislation is not minimized and specific rules are set in stone, data protection policy cannot effectively evolve. Continued experimentation and analysis is necessary before any federal law regarding data protection should have dramatic preemptive effect.

#### **IV. DATA SECURITY REQUIREMENTS MUST BE INCLUDED AND PRESERVED IN BREACH LEGISLATION**

Data breach laws serve an important function in generating transparency and helping people respond when their information has been breached. But the effectiveness of breach notification in protecting personal information is limited. Under a pure breach notification scheme, providing reasonable data security is voluntary. Companies protect data to the extent they minimize the risk of a reputational and financial penalty associated with notifying its customers of a breach. This risk calculation will be different for all companies. Not all companies fear reputational penalties, particularly if the data they are holding is not that of their own customers.

We must not ask breach notification to do more work than it is capable of. Specifically, data breach law should not let data security be voluntary. If people cannot trust entities that collect and store our personal information, then commerce, innovation, public health, our personal relationships, and our culture will be significantly damaged. Therefore any data breach legislation must include requirements that all entities collecting personal data reasonably secure it.

Legislating data security protections is challenging because of the ever-evolving threats to personal information as well as the fact that data security protections are heavily dependent upon context. As a result, it is notoriously difficult to create specific data security rules that are broadly applicable. Any such specifications risk being simultaneously over-protective in some situations and under-protective in others. Thus, the best approach is to seek flexible standards amenable to clarification and modification over time. Additionally, data breach legislation should ensure that multiple regulatory bodies create and enforce data security policy. Legislation reducing both expertise and available resources to protect data would make people more vulnerable to data breaches.

#### **A. The FTC Should Have Rulemaking Authority for Data Security**

The FTC’s regulation of privacy and data security under Section 5 of the Federal Trade Commission Act has served a critical function for the U.S. system of data protection. Under this statute, “unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”<sup>10</sup> The FTC has used this authority to regulate companies under theories of deceptive promises of data security and unfair data security practices.

Starting with its first privacy-related actions in the late 1990s, the FTC has evolved into the most important data protection agency in the United States. The FTC plays two critical roles within the U.S. data protection ecosystem. It fills significant gaps left by the patchwork of statutes, torts, and contracts that make up the U.S. data protection scheme. The FTC also stabilizes the volatile and rapidly evolving area of data protection and provides legitimacy and heft for the largely sectoral U.S. approach to data protection.

The FTC has been effective using a case-by-case approach under Section 5. However, the agency is limited because although the FTC has specific rulemaking authority under COPPA and GLBA, for Section 5 enforcement—one of the largest areas of its jurisprudence—the FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective.<sup>11</sup>

Specific rulemaking authority for data security would have several benefits. Rules would help the FTC further clarify data security standards in combination with its data security complaints. The FTC’s current jurisdiction under Section 5 is limited to commercial entities. An effective grant of rulemaking authority would also cover non-profit entities and entities not engaged in commerce, such as educational institutions. Finally, effective

<sup>10</sup> 15 U.S.C. § 45(a)(1).

<sup>11</sup> Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C. §§ 45–46, 49–52, 56–57c, 2301–2312 (2012)).



data security rulemaking authority for the FTC would also include the ability to issue civil penalties against companies that fail to provide reasonable data security.

A reasonableness standard is thus far the most desirable for regulating data security. Most data security laws adopt some form of a reasonableness standard. What constitutes reasonable data security is determined by context and industry standard practices. Deference to industry keeps regulators from promulgating data security rules in an arbitrary and inconsistent way. This approach builds upon the formidable and evolving body of knowledge in the data security field and common data security practices. There is a consensus that custodians of personal information act unreasonably when they fail to identify their assets and risk, minimize collection and storage, implement administrative, technical, and physical safeguards, and develop data breach response plans.

#### **B. Multiple Regulating Bodies Should Be Responsible for Data Security**

Numerous federal agencies require data security from companies in some form, including the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Department of Health and Human Services (HHS), the Securities and Exchange Commission (SEC), and the Food and Drug Administration (FDA). Other agencies, such as the Federal Aviation Administration (FAA) and the National Highway Transportation Safety Administration (NHTSA) have been encouraged to regulate data security in new technologies such as drones and automated cars. These agencies are not redundant in regulating data protection. Rather, they can and do coexist with unique expertise and regulatory authority. Even agencies with overlapping jurisdiction contribute valuable resources and have relatively harmonized approaches to data security.

Data security is not just a national issue. It is also a local issue, sometimes affecting a small but significant group of state residents. Even in the case of large, national breaches, residents of some states are hit harder than others. Federal data breach legislation must preserve the ability of states to regulate data security. States are nimble and capable of continued experimentation regarding the best approach to regulating data security. They are also closer to those whose data was compromised. Finally, states provide additional resources to alleviate the strain and cost of enforcement on federal agencies.

#### **V. CONCLUSION**

Sound federal data breach legislation should provide better transparency, more robust data security, and more effective remedies for individuals affected by a breach. However, legislation that replaces strong consumer protections with weaker ones, creates gaps in protection, and frustrates the ability for data protection law to evolve will do more harm than good. The modern threat to personal data is still relatively new. The concept of data breach legislation is newer still. It is too early to start rolling back protections and consolidating agencies to cut costs. Instead, sound data breach legislation should reinforce the current trajectory of data protection law which involves multiple approaches and constantly evolving robust consumer protection.

Mr. BURGESS. The gentleman yields back, and I thank all the witnesses for their testimony and participating in today's hearing. We will now move into the question-and-answer portion of the hearing, and for that purpose, I will recognize myself for 5 minutes. And I do again thank you all for being here.

Let me just ask a general question to the entire panel, and we will start with Ms. Hyman and work our way down to Ms. Hartzog. Reading through the testimony and listening to you this morning, it is clear that most of the panelists agree on—I guess I could say three out of four panelists agree on preemption, that it is necessary for a successful piece of legislation on data security and breach notification. The question is why is it important to have a single standard rather than allowing new requirements to be developed in State courts on top of a Federal law? Ms. Hyman, let us start with you.

Ms. HYMAN. Thank you, Chairman Burgess. It is important because right now we have all these different laws, many of which are in conflict with one another. Many of our member companies are small- and medium-sized IT firms, and they are trying to do business across State lines. They don't necessarily have the in-house resources to cover all the different State requirements. So having a more simplified Federal standard, strong but a Federal standard, would allow these companies to do business across State lines with confidence that they are serving their consumers.

The only other thing I would point out is, and I mentioned this in my opening remarks, this is a very unsettled area. As I mentioned just in the last couple of weeks, we have seen a number of bills introduced in State legislatures, and again, if there is some way that we can come up with a strong, appropriate Federal standard, I think it would alleviate a fair amount of ambiguity for both the consumer and for the business.

Mr. BURGESS. Thank you. Mr. Dodge?

Mr. DODGE. So I would say the States deserve a lot of credit for acting in the place where the Federal Government hasn't yet. But if Congress intends to or chooses to pass a Federal standard, we believe it should be preemptive because first, it will allow consumers to have a clear set of expectations regardless of where they live about what kind of notification they will get, at what time post-breach. We think that is important. Consumers need to know what to expect in the wake of a breach. And also for a breach of institution or business, they want to put all of their energy towards making sure they are quickly communicating actionable information to the consumers. And a national standard would allow them to do that instead of the complexity of complying with 47-plus different laws.

Mr. BURGESS. Ms. Glasgow?

Ms. BARRETT-GLASGOW. Breach notification laws that are in place today in the States vary widely as has been said, and in some instances, we don't even have a security requirement in certain State laws. So enacting a Federal law that includes both a security requirement and a breach notification requirement will raise the level across the country. And I think if you study those laws to any great degree, you will find that there are very few exceptions that would make a State regime more protective from any consumers.

Secondarily, from a consumer perspective, we don't live in one State all our lives often. I grew up in Texas and moved to Arkansas. And different States with different regimes with different requirements for the types of notices that need to be given create inconsistency for the consumer if they happen to have received a notice in one State and then receive a different notice in another State. As I said in my testimony, I hope that we will look at much more cooperation between law enforcement and companies to educate consumers about the risks that are out there so that they can help in protecting themselves and not rely solely on companies or Government notifying them when there has been a problem.

Mr. BURGESS. Thank you. Mr. Hartzog?

Mr. HARTZOG. So I think that preemption on a very limited scale could actually be useful. I think the important thing to remember is that preemption is not an all-or-nothing game, right? So we can preempt minimally or we can have aggressive preemption. So one of the reasons I recommend minimal preemption is so we can move closer towards having a national standard but then preserve some of the hard-won consumer protections and also make sure that Federal legislation doesn't create gaps that things that were protected are no longer protected, so for example, solely interstate, intrastate data breaches. And I think that as far as the differences between the 47 different pieces of legislation, they do vary, but I think that maybe sometimes the differences can be overstated possibly. I mean, I think that sometimes it is compared so that it is apples to oranges, which I don't think is true. I think the more appropriate metaphor might be Fuji to red delicious apples, and the idea that it is very burdensome to comply with all 47 State laws, I think that is also possibly, potentially an overstated claim in the sense that (a) businesses comply with 50 different State laws all the time, and (b) a very robust support network exists to provide companies of all sizes with the adequate help they need to respond to data breach requirements.

Mr. BURGESS. I thank the gentleman. The Chair now recognizes Ms. Schakowsky, 5 minutes for the purposes of questions.

Ms. SCHAKOWSKY. Thank you. Professor, I wanted to direct my question to you. Authors of some State laws and some Federal legislative proposals have chosen to require notification to consumers to be determined by a standard in which notification is dependent on the presence of a risk of harm or actual financial harm to consumers. And I am just wondering if you are concerned about harms beyond identity theft, fraud, or other economic loss, and if so, if you could give us some examples that might narrow too much the definition of risk.

Mr. HARTZOG. Sure. Thank you very much. I think that the harm trigger as it has been described, the idea that you only have to notify if there is some kind of finding of harm, is a dubious proposition in several different ways, mainly because the concept of harm within privacy law is hotly contested, and to limit the idea of harm to something like financial harm I think is really constraining because there are lots of different harm that can result from data breaches. So fraud and identity theft are not the only two. When health data gets stolen, you risk things like discrimination, adverse employment decisions, emotional distress. The Sony

hack made it very clear that sometimes when information is breached, it is not used to commit financial harm. It is posted online for everyone to see.

And so that brings me to my next point which is the harm trigger is dubious mainly because it is very difficult to draw a line of causation between a breach that occurred and likely harm that can happen sometime in the future. So it is not as though data gets stolen and it is a one-to-one that harm occurs as a result of it. Oftentimes data gets flooded downstream and aggregated with other pieces of data, and it can be extremely difficult to meet the burden of proof that harm is actually likely in any one particular instance. And when you mandate a harm trigger in notification, then what that means is if you don't have enough information to prove some kind of likelihood of harm, which is often the case in many different kinds of data breaches, then the harm doesn't go out. So as a matter of default, the notification isn't extended.

And so I think that it is important to remember the many different ways in which harm can occur and the many different ways in which harm is a relatively dubious concept within data breach law, not the least of which is that we haven't even talked about the ways in which information can be used against people, not just to harm you for identity theft purposes but to trick you into revealing more information. This is a common phishing attack, right, which is what they call where they use your own personal information into tricking you into think this is a communication from a trusted source. You click on it, then disclose more personal information. And this is more than just a threat to the individual who is tricked. One of the most common ways to hack into companies is through exploiting human vulnerabilities, and one of the ways in which we do that is we take information about people and use that to trick them into revealing more information.

Ms. SCHAKOWSKY. Answer a question then. Is there a way to identify harm or define harm that would include everything you are talking about? Or are you saying that a harm trigger itself? In other words, what you are suggesting is there needs to be notification of a breach without having to establish harm at all or are you saying we need to define harm better?

Mr. HARTZOG. That is correct. So generally speaking, I want to caution against overleveraging the concept of harm, and the easiest way to overleverage the concept of harm is to create a harm trigger. And so as a result, my recommendation would be to have the default be noticed because any definition that you use to come up with harm is probably going to be pretty flawed. It is either going to be overinclusive in which it would include every single possibility of harm we can imagine, or it is going to be underinclusive and leave out huge chunks of things that we want to protect against.

And so as a result, my recommendation would be let us not overleverage the concept.

Ms. SCHAKOWSKY. I know in the Sony breach we saw employment records, for example, that were revealed. And so, you know, that would be I think a problem for a lot of people.

Well, let me just put this on the table, and maybe others would want to answer it at some other point, the concern that there would be some sort of problem of overnotification.

Mr. HARTZOG. The problem of overnotification is also one that I think can tend to be overinflated. So of course you don't want consumers and people getting 45 emails a day saying, oh, hey, guess what? You know, another piece of your data has been breached. But I think we are a very long way from reaching some kind of point where consumers would just flippantly ignore some kind of piece of advice and—

Ms. SCHAKOWSKY. I am going to go ahead actually and cut you off because my time has expired, but I thank you.

Mr. BURGESS. The gentlelady yields back. The Chair now recognizes the vice chair of the full committee, Ms. Blackburn, 5 minutes for questions, please.

Mrs. BLACKBURN. Thank you so much, Mr. Chairman. I want to talk a little bit about doing a technology-neutral data security requirement, and it seems like when we talk about privacy, when we talk about data security, when we talk about entertainment delivery, more and more we are hearing, you know, don't get specific on the delivery system or don't get specific on the technology because it takes us forever, forever, to bring legislation into line with where technology is.

So we are going to start. Mr. Hartzog, I will start with you. We will go all the way down the panel, and I just want to hear your thoughts on technology-neutral or specific and how you think we are best served to approach that.

Mr. HARTZOG. I would agree with you that we should strive to be as technology-neutral as possible. We have seen time and time again when we pass laws that are highly technically specific that they are almost outdated the moment they are passed. And so—

Mrs. BLACKBURN. They are.

Mr. HARTZOG [continuing]. This is why things like reasonable data security standards tend to make sense, and it also is another good strong word of caution against really being overly specific in any one particular area, and if to the point where you have to be overly specific, being sure that you have enabled the definition to change where possible. So I would agree.

Mrs. BLACKBURN. OK.

Ms. BARRETT-GLASGOW. I agree that the bill should be technology-neutral. I think a good example of language regarding security is the Gramm-Leach-Bliley security provisions which have now stood the test of 15, 16 years or so in the marketplace.

And I would also, which actually may touch on Ms. Schakowsky's question a little bit, in the Rush bill, H.R. 2221, the definition of harm reads determination that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. And I think that other unlawful conduct picks up a lot of opportunities as technology involves, as new unlawfulness occur, for us to not have to come back and revisit the language.

Mrs. BLACKBURN. Got it.

Mr. DODGE. So we would agree, of course, that we should be technology-neutral. I don't think we can ever lose sight of the fact that the criminals in this space are highly sophisticated and rap-

idly evolving as we have seen in some of the more recent reports, sometimes backed by nation-states. So allowing businesses to evolve as the threat evolves is really important, and technology is a big part of that.

Mrs. BLACKBURN. OK.

Ms. HYMAN. And we would agree as well, technology-neutral is an important principle. You know, we have gone from simple redaction to encryption to more sophisticated versions, and as has just been pointed out, you know, we have to keep ahead of those that wish to cause harm. And the innovation of the private sector is a great opportunity to lead on behalf of the consumers.

Mrs. BLACKBURN. OK. Thank you. Now, Ms. Hyman, we are going to stay with you and come right back down the row. When we are talking about preemption language, I want to hear—and this is the lightning round. We have got a minute and a half left on the clock. So what language do you want to see us consider as we look at preemption?

Ms. HYMAN. Well, as I stated previously, we want to make sure that we are not just ending up with the 48th standard—

Mrs. BLACKBURN. OK.

Ms. HYMAN. —that it needs to be strong enough to actually matter in terms of preemption and simplification.

Mr. DODGE. A strong preemption sets a single, national standard.

Mrs. BLACKBURN. OK.

Mr. DODGE. Again, States deserve credit for the work they have done, but you can't create a 48th law.

Ms. BARRETT-GLASGOW. In my written testimony, I actually suggested some language that you might want to take a look at. I am not going to get into that right here.

Mrs. BLACKBURN. Thank you.

Mr. HARTZOG. My recommendation would be preemption that served as a floor but not a ceiling and at worst would only preempt the very specific provisions listed by the Federal legislation.

Mrs. BLACKBURN. OK. Thank you all. I yield back.

Mr. BURGESS. The gentlelady yields back. The Chair now recognizes Ms. Clarke for 5 minutes for your questions, please.

Ms. CLARKE. Thank you, Mr. Chairman, and I thank the ranking member. I would like to drill down a bit more on the breach notification issue.

Breach notification laws and legislative proposals can vary greatly in how they treat the question of when a company affected by a breach is required to notify consumers. The Data Accountability Trust Act, H.R. 2221, affirmatively presumed a company affected by a breach would notify consumers in the breach unless it determined that there is a reasonable risk of identity theft, fraud, and other unlawful conduct. There have also been proposals with a “negative presumption,” in other words, that a company does not have to notify consumers unless an investigation reveals that a certain level of risk exists to the consumers whose information was breached. The burden to prove risk in this case is not on the breached holder of consumers’ personal information but rather on those challenging its breach notification practices.

So Professor Hartzog, have you thought through what should be the presumption for firms to notify consumers of a breach and if so, why?

Mr. HARTZOG. Thank you very much. I have, and my recommendation would be to a presumption of notification in terms of breach. There are some interesting options available with respect to granting a safe harbor that are still debatable. Maybe if you make information unusable, unreadable, using things like encryption standards, then that is something that States have been experimenting with. That is a positive element, although that is not free from controversy with respect to the effectiveness of encryption. But when the presumption is that you don't have to notify unless an assessment of risk of harm proves that it is likely, then you miss out on a great deal of notifications. And it is important to remember that notifications are important not just for the individual that is being notified but also for other companies that are similarly situated so that they can know about threats that are facing them and perhaps practically respond to them, for State AGs, for the public so that they can be aware, just become more aware of the issues about data breach generally speaking.

So when the default is set and a practical effect will result in far fewer notifications, then I think that the public and other companies and individuals are——

Ms. CLARKE. So that brings me back around to the question raised by Ranking Member Schakowsky. She broached this issue of overnotification with you, and one of the concerns raised about breach notification is notification fatigue or overnotification. Would a negative presumption for notification be effective in preventing overnotification?

Mr. HARTZOG. I think that it is not so much as to whether the presumption of harm trigger would be effective in preventing overnotification. Certainly it would probably result in fewer notifications. So then the question becomes is that a good thing or a bad thing? And I again state that we collectively lose out when notifications drop, even though there have been breaches because there is value we can get from notification. And also, overnotification is a problem not just aided by reduction in notification, but we also need to continue to experiment with the way notification is given. There is a presumption maybe that notification is just a big dense block of text that individuals would—it is very easy just to look at and throw in the trash. One of the reasons we still need to experiment, perhaps at the State law level, is that we need to focus on the way notification is actually delivered because there is a lot of opportunity there to avoid oversaturation as well.

Ms. CLARKE. Did any of you want to weigh in on the issue of overnotification or concerns that your industries may have? Ms. Glasgow?

Ms. BARRETT-GLASGOW. Yes. I will go back to H.R. 2221, and the language that is in there I think is reasonable and good in terms of both the risk of harm as well as the presumption of notification unless it says the person shall be exempt from the requirement, meaning the notification, if certain conditions apply.

I think we have to be very careful about overnotification. I think we have learned through not just breach notification laws that

exist today but also other requirements such as Gramm-Leach-Bliley privacy notices that when consumers get repeated information about risks or about even what a bank may do with their data and there is no clear instruction as to what to do, and there may not be any recourse other than watch your accounts, that is possible, then they tend to get far more complacent about them and potentially even not read the one that really was the one that they needed to react and respond to. So I think industry in general is very sensitive to the overnotification problem.

Ms. CLARKE. Let me just say very quickly in closing, is there something that we can learn? Is there value to proceeding with notifications simply in terms of uncovering what works best? We are really in the advent of understanding exactly what is taking place. We wanted to get a sense of whether in fact there is value. Mr. Hartzog?

Mr. HARTZOG. One of the great benefits of breach notification statutes is it allows us to collect information and then issue reports which could then benefit not only companies but the field of data security generally because it helps us know where threats are coming from, what the response to those threats are, and how long it takes to respond.

Mr. BURGESS. The gentlelady's time has expired. The Chair thanks the gentlelady. The Chair now recognizes the vice chair of the subcommittee, Mr. Lance, for 5 minutes for questions, please.

Mr. LANCE. Thank you, Mr. Chairman. This is a very complicated issue, and we don't want to become the 48th and yet we want strong protection. And I think it is going to be a difficult needle to thread.

Ms. Glasgow, as I understand your testimony, you believe that we threaded the needle relatively well in Gramm-Leach-Bliley, is that accurate?

Ms. BARRETT-GLASGOW. As in regards to the security rule, yes.

Mr. LANCE. Yes. And do other distinguished members of the panel have an opinion on that and how it might relate to what we are attempting to do here? Ms. Hyman?

Ms. HYMAN. As we think about harm and the risk of overnotification and how we should be looking at this, we want to make sure that the information that is exposed actually is significant harm. So just having for example a name or address on its own without other identifiable information like a Social Security, these things need to be seen in context, and how we thread that will be important.

Mr. LANCE. Mr. Dodge?

Mr. DODGE. So I think the regulatory regimes that cover businesses should reflect the businesses themselves, but specific to notification, I believe that consumers should have a strong expectation of how they would be notified if certain information, personally identifiable information, is lost regardless of the business itself. It should be based on the data.

Mr. LANCE. Professor Hartzog?

Mr. HARTZOG. I think the Gramm-Leach-Bliley safeguards protections have been quite effective. They are technology-neutral and recognize data security as a process rather than just a one-time thing. So I would say that that has been very effective.



Mr. LANCE. So this might be an area of agreement in the panel, and I think this subcommittee and then the full committee want to reach a point where we can report to the floor a bipartisan bill that moves the Nation forward.

It has been a long time since I went to law school, but do we look ultimately to fundamental principles of tort law, Professor Hartzog, as to what we should be doing here?

Mr. HARTZOG. I would caution against relying on tort law too heavily, mainly because tort law is entrenched in a harm-based mindset.

Mr. LANCE. That is why I asked the question.

Mr. HARTZOG. And we see that because of causation issues, because it is very difficult to prove that one piece of notification when compromised results in some kind of tangible harm on the other end. I teach tort law, and causation is one of the things you always end up getting tripped up on. And so I would actually caution away against looking to tort law and look into more general proactive regulatory principles.

Mr. LANCE. I was taught tort law by John Wade who is the reporter of the restatement in the law school not too far from where you teach, just a little north of where you teach. How about others on the panel regarding should we look at all to tort law or is it not broad enough given our desire in a bipartisan fashion to protect the public. Mr. Dodge?

Mr. DODGE. I know when I am out over my skis, so I wouldn't—

Mr. LANCE. I see.

Mr. DODGE [continuing]. Be able to comment on that.

Mr. LANCE. I see. Ms. Glasgow?

Ms. BARRETT-GLASGOW. No, I am a technologist, not a lawyer so—

Mr. LANCE. OK. That speaks well of you. Ms. Hyman?

Ms. HYMAN. Unfortunately, I have to join my colleagues on that.

Mr. LANCE. I see. I won't take all of my time, but let me say that the chairman and I have discussed this at some length, and we want to be able to report a bipartisan bill. But we don't want this to be the 48th State. We want to move the Nation forward, and we want strong consumer protection. And I know the chairman is dedicated to that as am I, and I hope that we can all work together. And I see some areas of agreement. Thank you, Mr. Chairman.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back. The Chair recognizes the gentleman from Massachusetts, Mr. Kennedy, 5 minutes for your questions, please.

Mr. KENNEDY. Thank you, Mr. Chairman. Thank you to the witnesses for testifying today. Insightful hearing. I want to build off actually some of the comments that my colleague, Mr. Lance, just talked about and touched on and try to see if we can thread that needle a little bit.

As he indicated, 47 States, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have all enacted their own laws requiring notification of security breaches involving personal information. Some States, such as Massachusetts and California, have mandated strong requirements. California's data breach notification law requires that a person be notified when their encrypted

personal information has been or is reasonably believed to have been acquired by an unauthorized person, and the consumer has the right to know about all breaches of personal information, not just those deemed capable of doing harm.

Massachusetts law mandates that data owners provide notice of a security breach to the State's Consumer Affairs Office, State Attorney General, and the affected resident and include any steps the data-holder has taken relating to the incident.

Professor Hartzog, some legislative proposals include preemption of "any provision of a law, rule, regulation, requirement, standard, or other provision having force and effect of law relating to either data security of personally identifiable information or notification following a breach of personal, identifiable information." As I understand it, that would not be limited to the 47 States' statutes but it could, building off of a comment a moment ago, also preempt tort law and contract law. Seeing as you are a tort professor, is that correct and can you just walk us through that a little bit?

Mr. HARTZOG. Sure. So that strikes me as very broad preemptive language and the kind of which I would recommend against, precisely because while tort law isn't our best hope, we still might actually find some hope in tort law, maybe not in the tort of negligence which is very harm based, but perhaps other theories. So some of the more successful theories at the State level with regard to data security have been promises made by companies about data security which is sort of a tort and contract mixture. And for legislation to preempt that I think would be very problematic, and I think we have to be very careful about broad preemption with respect to Federal sector-specific data security law as well because there are some extremely important protections that exist throughout in various different sectors.

And so that kind of preemptive language is exactly the kind of preemptive language that would strike me as one that would ultimately end up doing more harm than good based on how significant it would seem to scale back protections for consumers.

Mr. KENNEDY. So building off of that, Professor, as I understand it, Massachusetts data breach law has some strong data security requirements which include the authority of the Massachusetts Department of Consumer Affairs and Business Regulation to issue regulations regarding data security. Would those regulations then be preempted potentially by that language that I just referenced? We obviously, yes, don't want to add in another layer of regulation but want to make sure that there is some strong consumer protection standards and allow States to innovate here as well.

Mr. HARTZOG. That is correct. That language would seem to preempt the State law protections in Massachusetts as well as all the other States that have data security requirements related to it, and this is potentially problematic because while the general approach to regulating data security seems relatively consistent—we all want reasonable data security practices which are relatively tethered to industry standards—States and policymakers in general are still trying to figure out exactly the best approach to that. And it would seem to be a problem to set something in stone when we are still trying to grapple with this very important issue.

Mr. KENNEDY. OK. Thank you, Professor. I will yield back.

Mr. BURGESS. The gentleman yields back. The Chair recognizes the gentleman from Mississippi, Mr. Harper, 5 minutes for your questions, please.

Mr. HARPER. Thank you, Mr. Chairman, and thanks to each of you for being here. It is a great concern as to how you protect the consumers and reduce the burden here and maybe prosecute the bad guys. So there is a lot to be done. I don't know of a company that is not greatly impacted and truly troubled by this.

First question would be a follow-up, Mr. Dodge. Some have suggested that consumers should receive notice from the company that was breached, even if they have never interacted with that company. Wouldn't it be clear for a consumer if they receive notification about a breach from the company that they actually gave the information to directly?

Mr. DODGE. So we think that the obligation to notify creates a very important incentive to keep systems strong and protect the information that companies hold. We would urge the committee as it considers this to maintain that obligation but allow for flexibility for businesses to contractually determine the notifying party because I think there are situations that you describe where that is appropriate. But to try to contemplate all those situations would be problematic and could undermine that important incentive.

Mr. HARPER. Is there a risk to consumers that you could create some confusion by duplicate notification from the company they gave information to and also a third party? What do you say about that?

Mr. DODGE. So again, I think the objective from all the parties involved would be to make sure that it was a streamlined and clear notification. And so that is why we would argue that the value of maintaining that incentive is high, but allowing flexibility for the parties involved as you described to contractually determine who would distribute that notice.

Mr. HARPER. And this would be a question to Ms. Hyman, you, Mr. Dodge, and Ms. Glasgow. Some States trigger notification to individuals after the company determines that there has been an unauthorized access to their information while the majority of States require notice upon a reasonable belief that the data was acquired by an unauthorized party. So the data was actually removed from the system. Is there a danger of overnotification to consumers if the duty to notify individuals is triggered by access but not acquisition?

Ms. HYMAN. Yes, there is, and we think it is very important that companies have an opportunity to do an appropriate risk assessment to determine whether there has been actual access to the information.

Mr. HARPER. Mr. Dodge?

Mr. DODGE. We believe that it has to be at the time of the confirmed breach. You want to be able to, in the wake of a breach, to define the universe of affected individuals so that the notice goes to the people who truly were or could be impacted, rather than overly broad and catching people that perhaps weren't affected.

Mr. HARPER. OK. Ms. Glasgow?

Ms. BARRETT-GLASGOW. You know, the subtle difference between access and acquisition is really kind of lost I think in this debate

in that if there is access and it is from an unauthorized person, you more than likely have some potential risk.

So if a company is assessing that, I think responsible companies are going to err on the side of caution.

Mr. HARPER. And Ms. Glasgow, earlier you testified when we were talking about a national notification standard, you mentioned a harm-based standard. In your eyes, who is best able to determine if there is harm?

Ms. BARRETT-GLASGOW. Well, I think it is determined by a number of parties. First, the company is the one that is on the line to begin with to make that assessment based on their understanding of what has happened. But beyond that, there are various regulatory agencies, the FTC at the Federal level and of course State AGs at the State level, that put teeth into that analysis to make sure that that assessment is done effectively and fairly for all parties.

Mr. HARPER. Just as a comment. When you have 47 standards and you have a company, most companies are national companies. It is extremely confusing and difficult for them, and that is why as we look toward a bipartisan approach to this, it is going to be very important how we move forward.

Mr. DODGE, if I could ask you, while there are ongoing discussions on how to establish a sensible time period in which companies are required to notify consumers of a breach, I am also interested in understanding what exactly or who exactly would start the notification timeframe so there is no room for misinterpretation of when companies are required to notify consumers. I would imagine that your members would not want this left up for interpretation after the fact. What are your thoughts on when this clock should start and who should be responsible for starting it?

Mr. DODGE. So we believe that the trigger should be the confirmation of a breach, and at that point of course there are lots of players who would be involved from law enforcement to presumably regulators if Congress were to go down this path. I think what is important to remember that there needs to be flexibility in that timeline because there are a number of steps that need to occur in order to ensure that the notice that goes out provides actionable information. So you want to first define the universe as I said a moment ago. Then you need to train your staff because invariably when these notices are received, it is going to lead to a number of questions. It won't be limited to the phone number or whatever the method of contact is on the notice. So you need to train staff in order to be able to respond and help consumers protect themselves.

And then there is the complex process of sending out a notice. It could be extremely large scale and making sure that notices aren't just going into junk mailboxes.

Mr. HARPER. And not meaning to cut you off, my time is expired. Thank you, Mr. Chairman.

Mr. BURGESS. The gentlelady yields back. The Chair thanks the gentleman. The Chair now recognizes the gentleman from Vermont, 5 minutes for your questions, please.

Mr. WELCH. Thank you. I didn't know whether Mr. Rush was ahead of me or not, but he tells me he is not from Vermont. So I am OK to go. We would love to have you.

Thank you very much. This is extremely helpful. A couple of the issues we are wrestling with is, number one, is preemption, and in general, I favor nonpreemption but I have been persuaded that if we can get the right standard, this is one of those situations where it really makes sense to have preemption.

Let me just go down the line like my colleague, Marsha Blackburn, did. If we have preemption, it is going to give I think a lot more comfort to those of us who are willing to take that step if the standard is stronger, and we have got a strong standard in Illinois. We have got a strong standard in California. In my conversations with some folks in the industry, the advantage of a single standard makes them supportive of a strong standard. And I want to just get each of your views on that. In other words, if we have preemption, do you support a relatively robust standard?

Ms. HYMAN. We have spoken out in favor of significant harm to the consumer. States are justifiably proud of the work that they have done. The chairman of our IT security group is from Massachusetts, but he, too, has shared with us the notion that the patchwork has become unworkable——

Mr. WELCH. Right. So——

Ms. HYMAN [continuing]. For companies such as theirs. So——

Mr. WELCH [continuing]. You get a single standard, a strong standard is something you could support if you got preemption?

Ms. HYMAN. Yes.

Mr. WELCH. And how about you, Mr. Dodge?

Mr. DODGE. Again, based on the recognition in the case of harm or risk to consumers, yes, we totally agree, and we believe that the preemption is really, really critical.

Mr. WELCH. OK. Thank you. Ms. Glasgow?

Ms. BARRETT-GLASGOW. Yes, the harm-based trigger tied with Federal preemption is very acceptable.

Mr. WELCH. OK. And Mr. Hartzog?

Mr. HARTZOG. Well, I would say that if Federal legislation is really going to move the ball forward and not actually strip away existing protections, then we should not have a harm-based trigger, and we should also, even to the extent that we should have broad definitions of things like PII which we have now, that may actually change in the future. And so we need to be sure that we can change the law——

Mr. WELCH. If I understood your testimony, though, you had reservations about preemption, but you weren't categorically opposed to it.

Mr. HARTZOG. That is correct. That is right.

Mr. WELCH. Your concern is that whatever our standard is, it be robust.

Mr. HARTZOG. That is right.

Mr. WELCH. Correct?

Mr. HARTZOG. So, so long as the standard is at or above what we currently have now, then I think that we can continue to move in the correct trajectory for data breach.

Mr. WELCH. OK. Thank you for that. The other question is if you have a single standard, can you have that be enforceable at the local Attorney General level as well as at the Federal level? And folks like Illinois, the Attorney General has been very active in

this. I know Vermont has been active in local enforcement. Would there be any problem with allowing the enforcement of that standard, both at the Federal and at the State level, where people would have I think more confidence that they would be heard? Let us go down the line.

Ms. HYMAN. Sure. We understand and accept the notion that the State Attorneys General should have the opportunity to enforce or the FTC or the Federal body, but we would argue that one should extinguish the other. In other words, you shouldn't have those contemporaneously.

Mr. WELCH. I see. OK. Mr. Dodge?

Mr. DODGE. Just building off that, I think we do recognize that there is an important role for the State AGs to play in this.

Mr. WELCH. Thank you.

Ms. BARRETT-GLASGOW. Yes, I agree, and so long as the coordination between State AGs and FTC is in place.

Mr. WELCH. OK. Mr. Hyman [sic]?

Mr. HARTZOG. I would agree that enforcement of the State AGs would be desirable for a data breach.

Mr. WELCH. OK. The other question I want to go to is this whole issue of tort law, and I understand that is somewhat injected into this. My understanding is, and correct me if I am wrong, the issue of tort law just applies in general across commerce and across non-commercial activity, and this committee, I am not sure—fMr. Chairman, I thought you were correct in your opening statement for acknowledging in some areas we simply don't have the jurisdiction to get involved. And I am thinking—

Mr. BURGESS. Would the gentleman yield?

Mr. WELCH. Yes, I will.

Mr. BURGESS. For his purposes going forward, the Chair is always correct.

Mr. WELCH. That more or less settles it. But I see that this whole question of tort law and whether there should be some carve-out as really a separate question from the heart of this legislation. There are a lot of folks that would love to not ever have to worry about tort law, but that is across the whole spectrum of any kind of activity in society, and taking that challenge on in this legislation may be a burden that is inappropriate to bear and too great to bear.

So I just want to get your comment as to whether some tort provision in here in your mind is essential to getting some of the good things that both sides seem to be supporting.

Ms. HYMAN. Well, again, I will point out I am recovering lawyer. So my familiarity with tort law is a little bit obscured at this point in time. But the one thing I would say is that we need to separate out and distinguish between good actors and bad actors. And what this effort about data breach notification is about is trying to provide clear lines of responsibility between the companies and the consumer. There are always going to be people that are bad actors, and they should be punished.

Mr. WELCH. Right.

Ms. HYMAN. That is a different subject.

Mr. WELCH. OK. Mr. Dodge?

Mr. DODGE. I, too, am not a lawyer, so I can't speak to the details of tort law. But I would say that, you know, this whole exercise is about empowering customers, consumers, with expectations around how they would receive notice and empowering businesses to conform to a standard.

Mr. WELCH. All right. I see my time is expired. So the last two dodged the bullet. Thank you. I yield back.

Mr. BURGESS. The Chair thanks the gentleman. The Chair now recognizes the gentleman from Texas, Mr. Olson, 5 minutes for your questions, please.

Mr. OLSON. Thank you, Mr. Chairman, and congratulations on your first hearing of this important subcommittee, and welcome to all of our witnesses. I assure you, I went to law school, but you won't hear the word tort come out of my mouth through my questions.

Unfortunately, in today's world, data breaches are happening more and more often. Target, Home Depot, Neiman Marcus, Sony Pictures all have been attacked by very different bad actors. We have to be aggressive on account of this threat, but it is a bit but, we must craft a balanced approach that protects consumers without undue burdens upon business.

My first line of question is about notification. I want to bore down the issue a little bit. My first question to you, Ms. Hyman, is it realistic to require any company to notify consumers within a set number of days after a breach occurs?

Ms. HYMAN. Thank you, Congressman. First of all, I just want to reiterate, businesses are incented to be responsible to the consumer. This is about trying to make sure that the consumer has information quickly and it is actionable.

There needs to be a reasonable period of time to do a risk assessment to find out, as was pointed out by my colleague, was there actual harm? You know, are there opportunities to remedy that harm? What kind of messaging is being provided to the workforce so that they can respond to the consumer when a notice goes out? So a reasonable period of time needs to be in place for risk assessment. Thereafter, if there is an appropriate timeframe for the actual notification, that makes a lot of sense.

Mr. OLSON. How about if they have some notification, when did this breach occur? Wouldn't we say that is where it happened, that is where the notification period starts? I mean, I am so confused when this clock starts running. Any idea when that clock starts running, ma'am?

Ms. HYMAN. I think you are saying does the clock start—

Mr. OLSON. Yes, when does it start? You said it is reasonable.

Ms. HYMAN. When there is an actual breach.

Mr. OLSON. OK. When does it start if it is reasonable? When do we start the clock? When has the breach occurred?

Ms. HYMAN. As soon as there is any type of information for the company to take a look and do the risk assessment, they have to do that within a reasonable period of time.

Mr. OLSON. OK. Mr. Dodge, how about you, sir? Is there reasonable required notification within a set number of days?

Mr. DODGE. So we would urge flexibility in determining what that length of time is. As we have talked about, there are a number

of steps that need to occur. But in every instance, the business entity that I am aware of has a desire to communicate that quickly because they want to make sure they are limiting any exposure or risk to those affected by the breach itself.

Mr. OLSON. Ms. Glasgow, I know you are a UT Longhorn and probably want to talk about this issue. Any concerns about requiring notification of breaches?

Ms. BARRETT-GLASGOW. Yes. I think there are two. First, any kind of deadline tends to become the norm, and some breaches are a very simple or small breach. Notification can take place in a matter of days or weeks if it is contained, a briefcase that is lost or something that is easy to investigate.

A big, complicated breach like we saw with some of the recent ones that you mentioned, take much longer. And so, you know, we run the risk of extending a simple breach to 30 days because that is the rule. But we also run the risk of not having enough information to do the assessment. And the notification process may be iterative. Through an investigation, you don't always have all the facts immediately. I mean, think about any criminal investigation that law enforcement takes. You learn something, and from that you ask more questions and from that you ask more questions. So it can very much be an interactive process of learning over a fairly extended period of time. So I think any kind of arbitrary number is inappropriate.

You know, language like we suggested in our written testimony that says without undue delay we think creates the sense of urgency but doesn't necessarily penalize the very complicated investigation.

Mr. OLSON. And one final question about harmless breaches. We all agree that there are breaches that are harmless, yes or no? Ms. HYMAN, yes or no, harmless breaches? We agree that some breaches are harmless?

Ms. HYMAN. Yes, there are some harmless breaches because of the type of information that is accessed.

Mr. OLSON. Mr. Dodge?

Mr. DODGE. Yes, of course there are situations where intrusions can occur and no information has been taken.

Mr. OLSON. Ms. Glasgow?

Ms. BARRETT-GLASGOW. Yes. I will give another example and that is when the information that was taken is encrypted or is essentially in some form that is unusable by the thief.

Mr. OLSON. And Mr. Hartzog, Professor Hartzog?

Mr. HARTZOG. I would say it depended on how you define harm. There are lots of different ways to think about it. I mean, was the breach a result of poor security practices, even though it didn't result in financial harm? It resulted in perhaps a breach of trust. Even if it is rendered unusable, if the encryption standard—was it adequate to actually protect the data? And so I would actually hesitate from saying yes to that question simply because the way you define harm is everything and that—

Mr. OLSON. With you leaning yes, sir. I yield back.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman. The Chair now recognizes the former chairman of the subcommittee, my longtime friend, Bobby Rush, from Chicago.



Mr. RUSH. Thank you. Thank you, Mr. Chairman, and I want to also congratulate you on your first hearing. It is an outstanding hearing, and I want to congratulate all your witnesses. They have provided fine testimony. And Mr. Chairman, I am going to take your pronouncement under consideration that you are always right, that you are never wrong. No, you said you are always right. And I am going to really try to process that because I am never wrong. So we have come to some kind of mutual understanding and agreement on that, all right?

Mr. Chairman, I want to get to the matter of the day, and I want to talk Dr. Hartzog. Dr. Hartzog, I am of the opinion that somebody has got to be in charge of interpretation. Somebody has got to be in charge of implementation, all right? And I understand you call for regulation by multiple agencies in their areas of expertise. Beauty is in the eye of the beholder, and one of the issues that we are always struggling with in this place is who has got the final say? Who has got jurisdiction and what is it that they have jurisdiction over?

My question to you is, first of all, if you can kind of explain to us and clarify what do you mean by regulation by multiple agencies in their areas of expertise? Can you be a little bit more clear in regards to that? And my second question is do you believe that there should be one central agency who could be the final authority on data security for the Federal Government?

So will you try and clarify your perceptions in terms of jurisdictional issues?

Mr. HARTZOG. Sure. So thank you for the question. I think that there should not be one entity that is in charge of data security for the entire country simply because what constitutes good data security and reasonable data security is so highly dependent upon context and industry. And so we have already existing numerous regulatory agencies, like the Federal Communications Commission, HHS and HTSA, the FAA, many different regulatory agencies, all of which have in some form spoken and made some requirements for good data security or looking into requirements for data security. And it is imperative that we rely upon these multiple regulatory bodies because they have expertise in very specific things. So the Federal Communications Commission has well-developed expertise in regulating telecommunications companies, satellite companies, and cable companies and other intermediaries and the specific data security requirements that apply in those particular fields, which might differ than say a standard commercial enterprise.

That being said, sometimes there is overlapping jurisdiction, but what we have seen with multiple regulatory agencies is we have seen that they can coexist. They work together. Sometimes they have coordinated investigations. Sometimes they reach memorandums of understanding where they say, you know, you will handle certain kinds of data security breaches, and we will handle other kinds.

And so that is what I meant by the importance of regulatory bodies, multiple regulatory bodies.

Mr. RUSH. I have a second question here, and this is directed to Ms. Glasgow. The Federal Trade Commission called on Congress to

enact the legislation to allow consumers with access to information held by data brokers. The Commission has also recommended that one centralized Web site be created where consumers can learn about how their data is used, correction to inaccuracies of their data, and to opt out for marketing if desired. Do you support these recommendations?

Ms. BARRETT-GLASGOW. We actually have gone so far as to implement the recommendation to have one central site where consumers can come and look at the data that Acxiom holds and correct it and change it. And we continue to work with industry on whether or not having a central site where everyone lists themselves and a consumer goes there, how that might be effective in terms of transparency. We certainly support the objective that the FTC has stated relative to transparency.

Mr. RUSH. I only have a few seconds, but can you share with the committee some of your experiences? I mean, how do the consumers, how do they go about it? How do they grade their experience with Acxiom?

Ms. BARRETT-GLASGOW. Yes. The site requires the consumer to log in and identify themselves because we are going to be sharing the data that we have about them on that site. So we have to know who they are, but once they have logged in and established an account, then they can look at all the data that we used for any of our marketing products. They can delete an element. They can change an element, or they can completely opt out of the whole process online, and it happens in real time. We would encourage you to maybe go to the site and take a look. It is called AboutTheData.com.

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

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back. The Chair now recognizes the gentleman from Florida, Mr. Bilirakis, 5 minutes for your questions.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it very much, and again, thanks for holding this very important hearing, and I really thank the panel as well. This is so important to our consumers.

Consumers must be able to trust that information they provide. They want to make sure that it is safe. They provide the information to retailers, and the digital world where sales are increasing online—you know, this trust is vital to our economy. However, I do not believe such trust will be preserved by the current patchwork of laws. We need a stable law that ensures merchants are appropriately protecting consumers without sacrificing prosperity.

The first question is for Mr. Dodge. You mentioned in your testimony the benefits of the chip and PIN that we are transitioning to nationwide. However, my understanding is that a potential weakness exists for online transactions because the payment card is not actually present. Doesn't that mean that this technology and every other technology can be made obsolete by criminals that quickly adapt to new technologies? It seems to me that we need to ensure that what we pass into law meets the threat and is not prescriptive of one type of technology? Do you agree and what do you recommend?

Mr. DODGE. So just a couple of points first, specifically chip and PIN is not scheduled to be rolled out later this year. This has been a major point of tension between the merchant community and the financial services community because the expectation is the chip only is coming out. Chip and PIN has been in place around the world for many, many years and has been proven to dramatically reduce fraud. Retailers have argued for a very long time that we should be moving to this technology as quickly as possible because of its proven fraud protection and because in the context of today's hearing, that it has an important effect and devaluing the data that businesses hold. So the information that flows through a retailers system, at the point of sale, would be rendered useless to criminals if they were able to capture, if you use the chip and PIN system. We think it is absolutely critical.

To your point about evolving technologies, that is absolutely true. It is the best technology. Chip and PIN is the best technology that is available today, and we are years behind the rest of the world in catching up to it. And as a result, we are behind. When chip and PIN was introduced in Europe, we saw fraud flow in two directions, online in Europe to you point and to the United States because it became the lowest common denominator.

As for long-term solutions, we believe the chip and PIN serves a near-term need, and we need to evolve to next generation because as you suggest, the world is moving online. E-commerce is booming online.

Mr. BILIRAKIS. Thank you very much. The next question is for the entire panel. Some of the recent data breaches were caused by third parties, such as contractors. What recommendations would you make if any to address when these situations occur? We will start over here, if that is OK with Ms. Hyman.

Ms. HYMAN. Well, first of all, with regard to third parties, again, many of our member companies are solution providers, those third parties that you may be talking about. Human error continues to be one of the greatest causes of data breach, and I think doing best practices for the industry and for all companies involved on how to mitigate some of those human errors is very important. Education, ongoing efforts, we have an IT trust mark, security trust mark, which is a benchmark for an organization to undertake appropriate practices for data security. So all of these pieces come into play, but having a standard for data breach notification also puts everybody on notice about what the consumer needs to know in a timely and actionable way.

Mr. BILIRAKIS. Mr. Dodge?

Mr. DODGE. The questions about third-party—

Mr. BILIRAKIS. The third party, with regard to third parties, correct.

Mr. DODGE. Yes. So we think that it is important. It is important incentive that the breached entity be obligated to make the notice, but flexibility should exist for parties to contractually determine in the instance of a breach who should issue the notice.

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

Ms. BARRETT-GLASGOW. As a vendor, we see lots of increasing requirements from our clients to not only adhere to security stand-

ards but to have indemnification if a breach occurs in our environment of the data that we are holding and processing for them.

Mr. BILIRAKIS. Thank you. Mr. Hartzog?

Mr. HARTZOG. My recommendation would be maybe, if there is even a possible compromise here, which is if breached entities have no relationship to the consumer whose data they hold. Then perhaps there could be some kind of requirement where you would have to disclose the relationship—say, “We got this information from an entity that collected your personal information, which is why you don’t recognize us. But we were breached.” So that could be one way to handle that.

Mr. BILIRAKIS. OK, Mr. Chairman. I actually have one more question if you—

Mr. BURGESS. Ask unanimous consent that the gentleman be able to ask his question. Without objection, so ordered.

Mr. BILIRAKIS. Thank you.

Mr. BURGESS. It is an immense power that I wield here, Gus.

Mr. BILIRAKIS. OK, for the panel again, keeping in mind the touchstone of this process is notifying an individual in the event that they need to mitigate the economic risks associated with a breach, which entity is in the best position to notify individuals after a breach? Is there a reason to deviate from the structure that the States have used? And we will start with Ms. Hyman, please.

Ms. HYMAN. Are you asking in terms of who is responsible for the notification or which enforcement agency?

Mr. BILIRAKIS. Who would be responsible for the notification.

Ms. HYMAN. We want to make sure that we are, again, not over-notification or confusing the consumer. So that entity with which they have provided their information to that would have done the transaction would be the first source. Then contractually—and I come back to the previous question about third parties. There are contractual relationships beyond that.

Mr. BILIRAKIS. Again, with regard to the States, how would you—

Ms. HYMAN. We said that the State Attorneys General should have enforcement opportunities. If it is also the FTC that is undertaking enforcement, one should extinguish the other. They should not happen simultaneously.

Mr. BILIRAKIS. Very good. I am sorry. I am having a little trouble hearing. I apologize. Mr. Dodge, please.

Mr. DODGE. Sure. We strongly believe that the obligation to notify should be with the breached entity and then again, flexibility among parties to contractually determine who sends the notification, if it makes more sense for somebody else to send it. And we agree the State Attorneys General have an important role to play in this.

Mr. BILIRAKIS. Very good. Thank you. Please.

Ms. BARRETT-GLASGOW. In the interest of time, I will agree.

Mr. BILIRAKIS. OK. Very good.

Mr. HARTZOG. And I would agree that the current trajectory of the State law is what I would recommend.

Mr. BILIRAKIS. Thank you very much. I appreciate it. I yield back, Mr. Chairman. Thanks for allowing me to ask that last question.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman does yield back. Seeing no further members wishing to ask questions, I would like to thank the witnesses and members for their participation in today's hearing. Before we conclude, I would like to include the following documents to be submitted for the record by unanimous consent: a letter on behalf of the Consumer Electronics Association; a letter on behalf of the Direct Marketing Association; a joint letter on behalf of the American Bankers Association, the Consumer Bankers Association, the Credit Union National Association, Financial Services Roundtable, Independent Community Bankers Association, the National Association of Federal Credit Unions; an additional letter on behalf of the Marketing Research Association; a letter on behalf of the National Retail Federation; a letter on behalf of the National Association of Federal Credit Unions; a joint letter on behalf of the Consumer Data Industry Association, the Interactive Advertising Bureau, the National Business Coalition on E-Commerce and Privacy, and the National Retail Federation, the United States Chamber of Commerce; and a joint statement for the record on behalf of the National Association of Convenience Stores and the Society of Independent Gasoline Marketers of America.

Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record, and I ask the witnesses submit their response within 10 business days upon receipt of the questions.

Without objection, all of the statements are entered into the record.

And without objection, the subcommittee is adjourned.

[Whereupon, at 12:50 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]



Consumer Electronics Association  
1919 South Eads Street  
Arlington, VA  
22202 USA  
866-858-1555 toll free  
703-907-7600 main  
703-907-7601 fax  
CEA.org

January 27, 2015

Chairman Michael C. Burgess and Ranking Member Jan Schakowsky  
House Committee on Energy and Commerce  
Subcommittee on Commerce, Manufacturing, and Trade  
2125 Rayburn House Office Building  
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky;

The Consumer Electronics Association (CEA)® is the technology trade association representing the \$223 billion U.S. consumer electronics industry. Every day, our more than 2,000 member companies are busy innovating; creating new technologies and American jobs. At CEA, we work to advance government policies that allow these companies to thrive.

In an increasingly digital world, data is the lifeblood of commerce. Stolen data also has value to criminals who appropriate it for identity theft and other crimes, and the black markets that permit such information exchange are sophisticated. It is difficult for consumers to protect themselves in this environment despite the best efforts of businesses to implement preventative cybersecurity measures. Unfortunately, the reality is that cybercriminals will find ways to breach computer networks even while businesses implement more and more sophisticated defenses.

Consumers and law enforcement agencies stand a much better chance of mitigating the consequences of cyber-theft if they have sufficient notification. To date, we have relied primarily on a patchwork of 47 different state data breach notification laws. These laws, while similar in effect, can have significantly different requirements related to notification timelines, content of consumer notices, and responsibilities to consumers in terms of identity theft mitigation. This system is confusing to consumers and presents daunting complications for businesses, including potentially conflicting requirements for notification to law enforcement. Furthermore, consumers could receive different information at different times because of this piecemeal approach, creating even more stress and confusion for the consumer. We need a single, preemptive federal data breach notification standard that will streamline the process of consumer and law enforcement notification. Consumers, law enforcement, and businesses alike will be given the certainty they need to effectively combat the harmful effects of stolen data.



Consumers should be able to count on a clear and consistent notification process. Congress needs to act to ensure consumers in one state get the same information, on the same timeline, as consumers in another. Businesses can better protect and inform their customers with one federal data breach notification standard that preempts the patchwork of state laws. Without preemption, a federal standard is just one more layer of confusion for businesses and consumers.

CEA supports federal preemption for a data breach notification standard, and thanks the Committee for holding a hearing on this key issue. We urge a bipartisan solution that will best serve consumers, law enforcement, and businesses in mitigating the harmful impact of stolen data. We stand ready to work with the Committee as it moves a legislative solution forward.

Sincerely,



Gary Shapiro  
President and CEO



January 26, 2015

The Honorable Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing and Trade  
Committee on Energy and Commerce  
United States House of Representatives  
Washington, DC 20515

The Honorable Jan Schakowsky  
Ranking Member  
Subcommittee on Commerce,  
Manufacturing and Trade  
Committee on Energy and Commerce  
United States House of Representatives  
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

As the Subcommittee on Commerce, Manufacturing and Trade examines the issues surrounding data breach legislation tomorrow in its hearing titled, "What are the Elements of Sound Data Breach Legislation?," the Direct Marketing Association (DMA) and its members write to express our ongoing support for a uniform national standard for data breach notification. Protecting individuals' sensitive personal information from theft or illegal uses has been and will continue to be a top priority for the data-driven marketing community. Federal data breach notification legislation would help businesses by reducing the complexity associated with complying with 47 state data breach laws.

DMA is the world's largest trade association dedicated to advancing and protecting responsible data-driven marketing in the United States and globally. Founded in 1917, DMA represents thousands of companies that drive the information economy. DMA members have engaged in the responsible collection and use of data for marketing purposes for more than 100 years. These responsible and innovative data uses have revolutionized the delivery of products and services to their customers and fostered many additional consumer benefits, such as virtually limitless free Web content. According to a recent study, the resulting Data-Driven Marketing Economy (DDME) added \$156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in a single year.<sup>1</sup> In short, information and information-sharing has changed the everyday lives of most Americans and has significantly contributed to U. S. economic growth overall.

We agree that notification to affected individuals when data is compromised for illegal purposes is a vitally important issue for both businesses and consumers. To this end, we have worked collaboratively with Members of Congress in both chambers and on both sides of the aisle over the years to help identify a workable path toward passage of a federal data breach notification law. As discussions continue in the 114th Congress, we remain committed to supporting the enactment of legislation that will provide consumers with timely information and meaningful protections without unnecessarily hampering critical business operations. We believe that sound breach notification legislation should include these core elements:

- **State Preemption & Consolidated Enforcement.** We continue to believe that meaningful data breach notification legislation must establish a clear federal standard that preempts the patchwork of state laws in this area. Currently, disparate laws in 47 states plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands, frustrate efficient and uniform breach notification to consumers.

---

<sup>1</sup> Deighton and Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* (2013), available at <http://thedma.org/valueofdata>.



This is particularly true when a data breach affects individuals nationwide who reside in a number of the jurisdictions covered by these various laws. Enforcement of a uniform federal standard should also be consolidated under the appropriate federal government agency or agencies. However, we do not believe that the Federal Trade Commission should be granted additional civil penalty authority in this area.

- **“Significant Risk” Trigger.** Any federal notification regime should only be triggered by a breach event that poses a *significant risk* of identity theft or other economic harm to the affected individuals. We remain concerned that an overly-broad trigger would cause consumers to be burdened with unnecessary notifications that could ultimately lead to consumer complacency when a truly actionable breach occurs.
- **Sensible Definition of Sensitive PII.** A definition of sensitive personally identifiable information (sensitive PII) broadly drawn – one that captures non-sensitive data elements such as consumer information one might find in a printed or online telephone directory – could unnecessarily trigger notice when no real threat of identity theft or fraud exist. A balanced bill would also exclude public records and information derived from public records from its scope.
- **Timely Notice.** As we have learned from several recent data breaches, businesses are best equipped to protect and notify consumers when they are provided sufficient time to gather the facts, secure their systems, and work with law enforcement before prematurely notifying the public. Initial breach detection, the restoration of system security, and a forensic analysis to determine which data may have been compromised and which customers may be affected are necessary but complicated tasks that often take months to complete. However, we do believe that businesses should always act to notify consumers *without unreasonable delay*, and, if additional time is required to complete what often becomes a criminal investigation, then law enforcement involved in helping companies track down criminals responsible for the breach should not have their investigation compromised by premature public notification.
- **No Private Cause of Action.** Given the complexities of both data breach response and notification – often layered with the added complication of an ongoing criminal investigation – we believe that a federal notification standard should not allow for a private right of action.

We need Congress to act now to enact legislation that will help businesses effectively inform and ultimately protect the customers they serve when data compromises do occur.

We look forward to working with you on these important issues.

Sincerely,



Peggy Hudson  
Senior Vice President, Government Affairs  
Direct Marketing Association

CC: Members of the House Subcommittee on Commerce, Manufacturing and Trade

January 23, 2015

Chairman Michael C. Burgess  
Subcommittee on Commerce,  
Manufacturing and Trade  
Committee on Energy and Commerce  
United State House of Representatives  
Washington, D.C. 20515

Ranking Member Janice Schakowsky  
Subcommittee on Commerce,  
Manufacturing and Trade  
Committee on Energy and Commerce  
United State House of Representatives  
Washington, D.C. 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

Thank you for holding a timely hearing entitled, "What are the Elements of Sound Data Breach Legislation?" in the Subcommittee on Commerce, Manufacturing and Trade.

As the 114<sup>th</sup> Congress engages in public debate on the important issue of data security, the undersigned financial trade associations are writing this letter for the hearing record to: 1) give our perspective on the key elements that should be included in any legislative approach; and, 2) to make you aware of the current robust regulatory regime already in place that requires financial institutions to protect the financial information of their customers/members and to notify them in the event of a breach that is likely to put them at risk.

We share your concerns about protecting consumers and strongly believe that the following set of principles should serve as a guide when drafting legislation to provide stronger protection for consumer financial information:

1. Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security regime, applicable to any party with access to important consumer financial information.
2. Banks and credit unions are already subject to robust data protection and notification standards. These Gramm-Leach-Bliley Act (GLBA) requirements must be recognized.
3. Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification standards.
4. In the event of a breach, the public should be informed where it occurred as soon as reasonably possible to allow consumers to protect themselves from fraud. Banks and credit unions, which often have the most direct relationship with affected consumers, should be able to inform their customers and members about the information regarding the breach, including the entity at which the breach occurred.
5. Too often, banks and credit unions bear a disproportionate burden in covering the costs of breaches occurring beyond their premises. All parties must share in protecting consumers. Therefore, the costs of a data breach should ultimately be borne by the entity that incurs the breach.

As noted above, some industries – including the financial industry – are required by law to develop and maintain robust internal protections to combat and address criminal attacks, and are required to protect consumer financial information and notify consumers when a breach occurs within their systems that will put their customers at risk. The same cannot be said for other

industries, like retailers, that routinely handle this same information and increasingly store it for their own purposes. The Identity Theft Resource Center has compiled a list of ***all publicly reported breaches in the United States*** and shows that banks accounted for only 5.5 percent of all breaches in 2014. Other businesses accounted for 33 percent. Retailer groups continue to cite a Verizon report on data breach statistics as a way to distract policymakers regarding the primary focus of data security breaches, but the inconvenient truth is that this Verizon report is based on an ***international sample*** of breaches as opposed to an actual compilation of all publicly reported breaches in the United States.

For more than 15 years, credit unions and banks have been subject to significant regulatory requirements and internal safeguards which have been substantially enhanced over the years. These include:

- Federal Requirements to Protect Information - Title V of the Gramm-Leach-Bliley Act and its implementing rules and guidance requires banks and credit unions to protect the security, integrity, and confidentiality of consumer information.
- Federal Requirements to Notify Consumers - Banks and credit unions are also ***required to notify*** customers whenever there is a data breach where the misuse of customer information has occurred or it is reasonably likely that misuse will occur.
- Strong Federal Oversight and Examination - Under their broad-based statutory supervisory and examination authority, the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration ***regularly examine*** financial institutions for compliance with data protection and notice requirements.
- Strong Federal Sanction Authority - Under numerous provisions of Federal law, banks and credit unions are ***subject to substantial sanctions and monetary penalties*** (e.g., up to \$1 million per day fines) for failure to comply with statutory and regulatory requirements.

***This extensive legal, regulatory examination and enforcement regime ensures that financial institutions robustly protect American's personal financial information.*** In contrast, retailers that accept electronic payments face no similar requirements or oversight, and as a result millions of American consumers' personal financial information has been compromised in recent years.

The groups below look forward to working with you and your colleagues in order to protect your constituents' personal financial information.

Sincerely,

American Bankers Association  
 Consumer Bankers Association  
 Credit Union National Association  
 Financial Services Roundtable  
 Independent Community Bankers Association  
 National Association of Federal Credit Unions  
 The Clearing House



January 26, 2015

**Hon. Michael Burgess (R-TX-26)**  
**Chairman**  
**Commerce, Manufacturing & Trade**  
**Subcommittee**

**Hon. Jan Schakowsky (D-IL-09)**  
**Ranking Member**  
**Commerce, Manufacturing & Trade**  
**Subcommittee**

**Re: Tomorrow's hearing on "What are the Elements of Sound Data Breach Legislation?"**

Dear Chairman Burgess and Ranking Member Schakowsky,

On behalf of the Marketing Research Association (MRA),<sup>1</sup> I write to share our views on data security legislation, the subject of your CMT Subcommittee hearing tomorrow. Spurred by the President's proposal, we hope you will (1) be careful in what kind of information gets covered by the bill, (2) avoid giving APA rulemaking authority to the Federal Trade Commission (FTC) to radically expand that definition, and (3) not set arbitrarily brief timelines for breach notification.

1. **Definition too broad:** The President's proposed definition for covered information ("sensitive personally identifiable information" in his draft) includes online account access information (e.g., usernames/passwords), which don't necessarily pose a security threat unless they provide access to truly sensitive personally identifiable information. Such types of data and combinations are not broadly recognized as posing a threat of ID theft and criminal abuse, and could lead to a slippery slope where most every piece of data could be covered.
2. **Too much FTC power:** Giving APA rulemaking authority to the FTC to alter that already too broad definition of "sensitive personally identifiable information," as the President proposed, would be a grave mistake. The agency would undoubtedly expand the definition radically. FTC Commissioner Ramirez<sup>2</sup> and others at the FTC have said that they consider almost any piece of data to ultimately be personally identifiable. The data covered by this bill is best determined by Congress, not an unelected and unaccountable regulatory body. Such radical expansion would result in more uncertainty for American employers, including survey, opinion and marketing research organizations, whose livelihood depends on the legitimate and accurate collection and analysis of information provided by consumers. The FTC would still be able to modify the definition using its regular Magnuson-Moss rule-making authority and we feel that should be sufficient to grapple with any major modifications to the definition that might be necessary over time.
3. **Arbitrarily short notice period:** The requirement in the President's draft to notify within 30 days of data breach discovery will be too short for some modern data breach investigations, which can be extremely complex and challenging. That is why laws usually require a "reasonable amount of time." By contrast, HIPAA has a 60 day limit.

We look forward to the Subcommittee's hearing tomorrow and working with the Subcommittee on a national data security bill that protects consumers without hindering survey, opinion and marketing research.

Sincerely,

Howard Fienberg  
 Director of Government Affairs  
 Marketing Research Association (MRA)

<sup>1</sup> MRA, a non-profit national membership association, represents the survey, opinion and marketing research profession and strives to improve research participation and quality. We keenly focus on data security and consumer privacy, since personal data is essential to the research process and our ability to deliver insights to clients.

<sup>2</sup> For example, at an [Energy & Commerce CMT Subcommittee hearing on July 15, 2011](#): "I think that the touchstone here is information that can be uniquely tied to an individual... broader than the definition that is currently used in the draft bill."



January 27, 2015

The Honorable Michael C. Burgess, M.D.  
Chairman, Subcommittee on Commerce,  
Manufacturing, and Trade  
Committee on Energy & Commerce  
United States House of Representatives  
Washington, DC 20515

The Honorable Jan Schakowsky  
Ranking Member, Subcommittee on Commerce  
Manufacturing, and Trade  
Committee on Energy & Commerce  
United States House of Representatives  
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

The National Retail Federation supports your efforts to craft effective data security breach notification legislation. We urge you to adopt a framework for a federal law that applies to all entities handling sensitive personal information and that would establish uniform, nationwide standards to ensure clear, concise and consistent notices to all affected consumers whenever or wherever a breach occurs.

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy.

For years, NRF has called on Congress to enact a preemptive federal breach notification law that is modeled upon the strong consensus of existing laws in nearly every state, the District of Columbia, Puerto Rico and other federal jurisdictions. A single, uniform national standard for notification of consumers affected by a breach of sensitive data would provide simplicity, clarity and certainty to both businesses and consumers alike. Importantly, a single federal law would permit companies victimized by a criminal hacking to devote greater attention in responding to such an attack to securing their networks and determining the scope of affected data and customers to be notified, rather than diverting limited time and resources of their legal team away to solve a patchwork of conflicting disclosure standards in over 50 jurisdictions. In sum, a federal breach notification law would ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.

As you know, American businesses of all types have suffered criminal intrusions that put their clients' and customers' sensitive data at risk. If Americans are to be adequately protected and informed, any legislation to address these threats must cover all of the types of entities that handle sensitive personal information. Exemptions for particular industry sectors that handle the same sensitive information would not only ignore the scope of the problem, but create risks criminals can exploit. A federal notice obligation applying to all breached businesses would also create significant

NATIONAL RETAIL FEDERATION  
1101 New York Avenue, NW, Suite 1200  
Washington, DC 20005  
[www.nrf.com](http://www.nrf.com)

incentives across industries to invest in technologies to better protect data and to respond appropriately to breaches whenever and wherever they occur. Federal legislation should, therefore, not leave any “notice holes” that allow businesses to avoid notification when they suffer a breach of their own system; doing so may not only leave affected businesses and customers unaware of a breach, but also creates disincentives to fully protect the data in their system if public notification is not required following a breach.

We look forward to continuing to work with you and the members of the Subcommittee to produce legislation we can fully support, and that Congress can enact, to establish uniform federal rules for the reasonable, timely notification to affected consumers by all businesses that suffer breaches of sensitive personal information.

Sincerely,

A black rectangular redaction box covering the signature of David French.

David French  
Senior Vice President  
Government Relations

cc: Members of the House Energy & Commerce Committee



3138 10th Street North  
Arlington, VA 22201-2149  
P: 703.842.2234  
F: 703.522.0594  
chunt@nafcu.org

National Association of Federal Credit Unions | [www.nafcu.org](http://www.nafcu.org)

**Carrie R. Hunt**  
Senior Vice President of Government Affairs  
and General Counsel

January 23, 2015

The Honorable Michael Burgess  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade  
Energy & Commerce Committee  
U.S. House of Representatives  
Washington, D.C. 20515

The Honorable Jan Schakowsky  
Ranking Member  
Subcommittee on Commerce,  
Manufacturing, and Trade  
Energy & Commerce Committee  
U.S. House of Representatives  
Washington, D.C. 20515

**Re: The Importance of Data Security to Our Nation's Credit Unions**

Dear Chairman Burgess and Ranking Member Schakowsky:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the interests of our nation's federal credit unions, I write to thank you for your efforts in taking steps to protect consumers from cyber and data security threats. NAFCU will closely monitor next week's hearing, "What are the Elements of Sound Data Breach Legislation?" as a chief concern of credit unions and their 100 million members continues to be data breaches at our nation's retailers exposing financial and personal data of millions of consumers.

As you know, consumers at risk in the wake of a data breach often rely on their credit union to help re-establish financial safety. In the process, credit unions suffer steep losses through the reissuance of cards, the charge-off of fraud, and the staff time it can take to respond to the magnitude of many of the breaches we have seen recently. Unfortunately, not all entities are held to a federal standard in protecting sensitive financial and personal information. While credit unions have been subject to federal standards on data security since the passage of *Gramm-Leach-Bliley Act* in 1999, the same cannot be said for our nation's retailers.

NAFCU member credit unions and their members have suffered greatly at the hands of negligent entities and have long sought legislation that would ensure retailers abide by a federal data security standard to better protect consumers. As your subcommittee looks at legislative solutions to address the data breach epidemic, we believe the following areas must be addressed:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

NAFCU | Your Direct Connection to Education, Advocacy & Advancement

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *Gramm-Leach-Bliley Act*.
- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.
- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.



Thank you for your attention to this important matter. We look forward to Tuesday's hearing and working with the subcommittee as you move forward in addressing data security issues. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Vice President of Legislative Affairs Brad Thaler at (703) 842- 2204.

Sincerely,



Carrie R. Hunt  
Senior Vice President of Government Affairs and General Counsel

cc: Members of the House Energy and Commerce Subcommittee on Commerce,  
Manufacturing, and Trade

January 27, 2015

The Honorable Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing and Trade  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Jan Schakowsky  
Ranking Member  
Subcommittee on Commerce,  
Manufacturing and Trade  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

The undersigned trade associations and business groups representing hundreds of thousands of U.S. companies from a wide variety of industry segments strongly supports enactment of a truly uniform national data breach notification law. Protecting individuals' sensitive personal information from theft or illegal uses has been and will continue to be a top priority for the business community. Federal data breach notification legislation would help businesses by reducing the complexity associated with complying with 47 state data breach laws.

As you continue drafting data breach notification legislation, we urge you to be mindful that any such legislation, to be workable and effective, must recognize that both consumers and U.S. businesses are victims of crimes that give rise to a data breach. To that end, we would like to take this opportunity to share with you our thoughts on specific provisions that should be included in the bill.

#### **Preemption**

We support a true national, uniform standard for data breach notification. With 47 states having already enacted data breach notification statutes, the only reason for Congress to act now is to expressly preempt obligations under related state and common laws to ensure uniformity of the federal act's standards and the consistency of their application across jurisdictions. A weak or poorly drafted preemption provision would accomplish little other than adding a new federal law to the state statutes and common laws already in effect, resulting in a confusing patchwork of requirements and enforcement regimes that would undermine the purpose and effectiveness of this legislation.

#### **Breach Notification Timing**

We agree that consumers should be notified in a timely manner after the occurrence of a reportable data breach. However, rather than specifying a specific timeframe, we recommend language—consistent with nearly all of the state breach notification laws—permitting greater flexibility given the complexities of responding to a data breach. All entities that suffer a breach, whether government agencies, nonprofits or commercial businesses, must first and foremost secure and restore the integrity of any breached system before notifying the public of their

vulnerability or else they will simply face continual cyber-attacks to further exploit the breached system. Additionally, breached entities must conduct extensive forensic analyses, often with the assistance of law enforcement, to determine which data may have been compromised and the identity of any potentially affected individuals. We therefore suggest the Subcommittee consider, as a model, the timeliness of notice provisions in S. 1193, in which notifications would be required to be made “as expeditiously as practicable and without unreasonable delay,” while permitting breached entities reasonable time following a breach to restore the integrity of their systems, determine the scope of the breach, and identify affected individuals to be notified.<sup>1</sup>

### **Enforcement**

If the FTC—acting on behalf of the federal government—exercises its right to enforce what would be federal law, then the states should be estopped from pursuing any action based on the “same or related acts” upon which the FTC prosecution is based. For example, S. 1897, adopts such a provision.<sup>2</sup> All enforcement actions should be filed in the appropriate federal district court.

When state enforcement is permitted, the legislation should only authorize an enforcement action under the new federal law to be brought by the state attorney general. The legislation should curtail the ability of state attorneys general to utilize contingency fee arrangements with private attorneys to enforce the Act or to litigate claims on behalf of their constituents.

### **Liability**

We urge you to recognize that an entity that suffers a data breach is often also the victim of a crime. Therefore, the main focus of any liability provision should be on the bad actor. Rather than applying a strict liability standard, the severity of the conduct must be a factor in assessing liability and any civil penalties. Specifically, we recommend that minor technical violations should not result in either civil penalties or liabilities. Given the complexity and expense of responding to a data breach, we caution that a flawed liability provision would further penalize an entity that is a victim of data breach by drawing away valuable resources necessary to fix the breach, notify customers, and augment existing security measures.

We look forward to working with you and your Subcommittee colleagues on this important legislation.

Sincerely,

Consumer Data Industry Association  
Interactive Advertising Bureau  
National Business Coalition on E-Commerce and Privacy  
National Retail Federation  
U.S. Chamber of Commerce

---

<sup>1</sup> Section 3(c) of S. 1193 (113<sup>th</sup> Congress).

<sup>2</sup> Section 203(c)(5) of S. 1897 (113<sup>th</sup> Congress).

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 ENERGY AND COMMERCE SUBCOMMITTEE  
ON COMMERCE, MANUFACTURING AND TRADE  
JANUARY 27, 2015  
“WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?”

Chairman Burgess, Vice Chairman Lance, Ranking Member Schakowsky and members of the subcommittee, thank you for giving us the opportunity to submit this statement for the record on the topic of the elements of sound data breach legislation. 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 is an international trade association composed of more than 2,200 retail member companies and more than 1,600 supplier companies doing business in nearly 50 countries. The convenience and petroleum retailing industry has become a fixture in American society and a critical component of the nation's economy. In 2013, the convenience store industry generated almost \$700 billion in total sales, representing approximately 2.5% of United States GDP.

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.

With this testimony, we will briefly lay out 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 the elements of data breach legislation that we consider to be most important. We also note that protecting against data breaches ought to be a primary focus given that notice laws have already proliferated around the country.

#### 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 22 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.

### 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 wrote recently, “The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history.”<sup>1</sup>

For example, 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 personal identification number (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.

The reason that financial institutions are not as interested in protecting against fraud on transactions with merchants than on transactions with financial institutions themselves is that those financial institutions push many of the losses from fraudulent transactions onto merchants. While the financial industry often claims that it provides merchants with a “payment guarantee”, it does no such thing. The Federal Reserve studied this a few years ago and found that, on debit transactions that did not use a PIN, merchants paid for more than 40 percent of fraud losses.<sup>2</sup> On credit card transactions, merchants pay for the majority of fraud losses. At our members’ gas pumps, for example, we pay for about 74 percent of fraud losses on debit and credit cards.<sup>3</sup>

<sup>1</sup> “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/>.

<sup>2</sup> 77 Fed. Reg. 46261, 46262 (Aug. 3, 2012).

<sup>3</sup> *Id.*

That is a major reason why PCI does not have the incentive to require the most effective security. The institutions that have the primary voice in PCI's work don't feel the full brunt of the economic consequences of their decisions.

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 during the past year – at banks and at merchants – have not involved the 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 PINs are required.

Requiring the use 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.

#### 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 that 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 2014 report (examining 2013 data) determined that there were 63,437 data security incidents reported by industry, educational institutions and governmental entities last year and that 1,367 of those had confirmed data losses. Of those with confirmed data losses, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, hotels and restaurants combined had 10%, and, 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.

### 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 51 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.

Many of these 51 laws are very similar. While there may be some benefits to streamlining this system by having one federal law that pre-empts these 51 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.

### Elements of Data Breach Law

There are several elements that we see as important to a federal law on data breach. First, the law should not have holes in it that result in consumers not getting notice. Second, 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, 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, the law should not take a punitive approach to businesses that have their data stolen by thieves. Fifth, if there is going to be a law, it should pre-empt state laws. There is no need for a fifty-second data breach law.

### 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 51 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.<sup>4</sup> GLBA guidance recommends that financial institutions have plans in place to provide consumer notification of data breaches, but again those plans are not required.<sup>5</sup> Following a breach, GLBA guidance says that banks should conduct an

<sup>4</sup> 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.

<sup>5</sup> 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



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.<sup>6</sup> 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.<sup>7</sup> 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.

Last August, JP Morgan Chase suffered the largest data breach in U.S. history. That breach was reportedly part of a pattern of breaches of financial institutions that included breaches of perhaps a dozen or so banks. In spite of this, only a few of the names of these banks have ever been reported. In fact, even the JP Morgan Chase breach became public only because there was a reference to it in a filing the bank made with the Securities and Exchange Commission. Once it became a front page story, JP Morgan Chase provided notice of its breach. It is not clear which of the other affected banks did the same. And, under GLBA, that appears to be just fine. In October, the USA Today reported that FBI officials had warned that 500 million financial records had been stolen from banks over the previous year. It is not clear how many of those incidents resulted in notice to consumers.

Thankfully, the majority of state laws help patch this major shortcoming in federal law. Based on our analysis, thirty-seven of the fifty-one state and territorial data breach laws cover banks while fourteen 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.

#### 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.

---

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*].

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

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.<sup>8</sup> 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 providers are “dumb pipes.” Nothing could be further from the truth. Data lines include switches and routers throughout them 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.

But these complexities are why the Federal Communications Commission and the Congress are considering 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.

Other businesses 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

---

<sup>8</sup> The Nilson Report, Issue 934, Sept. 2009 at 7.

live up to their responsibilities – and don’t simply pawn off those responsibilities onto smaller players with fewer resources.

#### 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. In fact, two-thirds of data breaches take months to discover.<sup>9</sup> 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.

#### 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.

#### 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 51 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 fourteen states that exempt them from their laws.

---

<sup>9</sup> 2013 Data Breach Investigations Report, Verizon.

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 51 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-second 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.

#### Data Security

One thing worth emphasizing here is that data breach notification should not be the first priority in this area. As noted, notice is well-regulated today. Our first priority would be to focus on preventing data breaches. Merchants, including NACS and SIGMA members, collectively spend more than \$6 billion per year just securing payment data.<sup>10</sup> Spending on all data security certainly exceeds this amount. Doing common-sense things like requiring PINs on payment card transactions, developing encryption and tokenization technologies that are effective (and open to all in the industry rather than creating competitive market problems), and increasing information-sharing with private industry and between the private sector and government are all measures that could demonstrably improve our ability to prevent data breaches in the first place. Many of the challenges in these areas stem from problematic standard-setting in the payment card arena and we would urge that particular attention be paid to those issues given the vulnerabilities that anti-competitive standard-setting has allowed to fester.

And, given the prevalence of foreign states in data breaches today, it may be time to more deeply examine to what extent our prism for viewing data security should be based on a national security model rather than a criminal justice model. It may be that, as with national security threats in the physical world, the resources available to data thieves are outstripping the ability of private businesses to individually deal with these threats. That is an issue that this and other committees ought to consider.

\* \* \*

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.

---

<sup>10</sup> "Credit Card and Debit Card Fraud Statistics," CardHub 2013, available at <http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/>.

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (202) 225-2977  
Minority (202) 225-3841

March 4, 2015

Ms. Elizabeth Hyman  
Executive Vice President  
Public Advocacy  
CompTIA  
515 2nd Street, N.E.  
Washington, D.C. 20002

Dear Ms. Hyman,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, January 27, 2015 to testify at the hearing entitled "What are the Elements of Sound Data Breach Legislation?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, March 18, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at [Kirby.Howard@mail.house.gov](mailto:Kirby.Howard@mail.house.gov) and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Michael C. Burgess  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment



**Responses to Additional Questions for the Record submitted by The Honorable  
Michael C. Burgess**

Elizabeth Hyman

Executive Vice President, Public Advocacy

TechAmerica, the public policy department of CompTIA

March 18, 2015

**1. The President recently called for a single, national standard for breach notification legislation. Do you have a response to the language he proposed? Please discuss.**

We appreciate the President's endorsement of a national breach notification standard, but we have some concerns about the specifics of his proposal, such as:

- 1) The definition of "Sensitive Personally Identifiable Information" should contain an exception for information accessible through public records;
- 2) The 30 day timeframe for notification may not be long enough for companies to conduct a thorough risk assessment;
- 3) The 30 day timeframe is similarly unrealistic for receiving an exemption if a risk assessment finds that there was no reasonable risk of harm from the breach;
- 4) It does not contain a provision allowing substitute notification should the breached entity not have necessary contact information;
- 5) It does not ban private rights of action.

We simply cannot support a data breach notification bill that contains, from our perspective, such significant shortcomings.

**2. Given the activity of States regulating data security in the last few years, is there a benefit for industry if Congress sets a national standard for reasonable data security. Would you support a preemptive reasonable data security standard? Please explain.**

There is absolutely a benefit for industry if Congress sets a national standard for data security, as long as that standard is reasonable. However, we do not believe that data security requirements should be specifically enumerated by legislation, and should instead be determined by the FTC with assistance from industry to determine a set of "best practices." While our testimony focused specifically on data breach notification, and not data security, we have similar concerns about companies', particularly SMBs, ability to comply with a complex web of conflicting state data security requirements. A national standard would protect consumers by putting data security requirements in place for the states that currently do not have them, and benefit the tech industry by providing a clear standard by which all companies must abide.

**3. Would your members support data security and breach notification legislation that does not contain preemption of State law?**

Quite simply, we would not support legislation that does not preempt State law. The primary reason we have advocated for a national standard is to alleviate the compliance burden for companies who have to comply with the 47 different state standards. If a federal standard does not preempt the state standard, it will not accomplish that goal and will instead merely function as a 48<sup>th</sup> standard atop which states can add their own requirements. Compliance would remain as difficult as it is in today's environment.

**4. How do you define preemption that would effectively eliminate the existing patchwork of State laws?**

We have never advocated for a specific definition of preemption, but have long-supported strong preemption language that would ensure that the federal standard is the only standard with which companies must comply for notifying consumers following a breach. As stated earlier, it must be made clear that states cannot add additional breach notification requirements atop the federal standard.

**5. How do you believe state common law should be treated in federal data security and breach notification legislation? Should it be preempted?**

Federal data security and breach notification legislation should preempt state common law to the extent that individuals cannot sue companies simply for failing to comply with the federal security and breach notification standards. However, federal legislation should not preempt state common law that falls outside the scope of the legislation. Protection of consumer data must be a priority for companies, and we must not strip away consumers' ability to protect themselves.

**6. Please explain the issues that could develop in the marketplace if a federal data security and breach notification bill does not preempt State law.**

As explained earlier, a bill that does not preempt State law will simply add more confusion to the marketplace than we already have today. It will add one more law to the massive list of State laws that companies must already comply with. Ultimately, it would serve very little purpose.

**7. Do you support allowing State Attorneys General to enforce a federal data security and breach notification law if the law preempts current State law? Are there other factors that should be considered in extending this enforcement authority?**

We absolutely support allowing State Attorneys General to enforce a federal law. Doing so would put more cops on the beat to help protect consumers. However, the law must ensure that companies cannot be punished at both the state and federal levels for the same violation of the statute.

**8. There was testimony during the hearing that companies undertake investigations after a breach is discovered. Please explain the steps of a data breach investigation and what information companies learn during this process.**

Once a company suspects a breach, the first step is likely to determine the source of the breach and if it's too late to prevent information from being accessed. A company must then attempt to determine what was accessed, when it was accessed, how it was accessed, who it was accessed by, what they might do with the information, and what can be done to prevent a breach from happening again. Then it must ensure that its system integrity has been restored. Often these steps involve bringing in outside consultants and/or law enforcement for assistance, and can be expensive and time-consuming. The last thing companies should have to worry about at this critical point in time is which particular state laws apply to this particular breach and how to comply with each and every one of them properly.

**9. The dangers of over notification for consumers in the long term have been outlined by States, companies and the Federal Trade Commission. Taking this into consideration, what should the risk trigger be for a company to notify individuals after a breach?**

We have long advocated that any federal framework should require notification only when there is a risk that harm has or is likely to occur. Requiring notification without some threshold of harm risks overnotification of consumers.

**10. If there is a deadline for notification following a breach, should the clock start after the breached entity has been able to secure and restore the breached system? How do the states approach this in their breach notification statutes.**

We have long advocated that statutes should not contain a specific timeframe for notification and should instead require notification "without unreasonable delay" or within a "reasonable" time. All breaches are different, and creating a single timeframe for all breaches could prove problematic in certain situations. However, if a specific timeframe must be enumerated, we would suggest that the clock start after the entity has been able to conduct a risk assessment and secure their breached system. The risk assessment could take anywhere from days to months, depending on the breach, and notification before the assessment is concluded could prove damaging to the breached entity.

Most states do not require a specific timeframe for notification, and instead require notification "without unreasonable delay" and/or "in the most expedient time possible," and acknowledge that it may take time for companies to determine the scope of the breach and restore their systems. When states have laid out a specific timeframe, we have found that most states require notification within forty-five days following the discovery of the breach.

**11. What are cyber attackers typically looking for when they attempt to breach your members' networks? Do you know if the purpose is typically to embarrass the consumer or to steal his or her information for financial gain?**



We reached out to a number of members for feedback on this question and didn't receive the same answer twice, so it seems as if there is not one clear purpose for cyber attacks. Embarrassment appeared to be less of an incentive than financial gain, but we heard everything from "just poking around" to attempting to take down a company, to identity theft, to gaining access to a company's infrastructure for other nefarious purposes. Cyber attackers have many different reasons for carrying out attacks, and any legislation should acknowledge this fact.

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (202) 225-2927  
Minority (202) 225-3641

March 4, 2015

Mr. Brian Dodge  
Executive Vice President  
Communications and Strategic Initiatives  
Retail Industry Leaders Association  
1700 North Moore Street, Suite 2250  
Arlington, VA 22209

Dear Mr. Dodge,


Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, January 27, 2015 to testify at the hearing entitled "What are the Elements of Sound Data Breach Legislation?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, March 18, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at [Kirby.Howard@mail.house.gov](mailto:Kirby.Howard@mail.house.gov) and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

  
Michael C. Burgess  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641  
March 4, 2015

Ms. Jennifer Glasgow  
Global Privacy and  
Public Policy Executive  
Acxiom Corporation  
601 East Third Street  
Little Rock, AR 72201

Dear Ms. Glasgow,


Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, January 27, 2015 to testify at the hearing entitled "What are the Elements of Sound Data Breach Legislation?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, March 18, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at [Kirby.Howard@mail.house.gov](mailto:Kirby.Howard@mail.house.gov) and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

  
Michael C. Burgess  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade  
Attachment

Subcommittee on Commerce, Manufacturing, and Trade  
What are the Elements of Sound Data Breach Legislation?

Response of:

Ms. Jennifer Glasgow  
Global Privacy and Public Policy Executive  
Axiom Corporation

Additional Questions for the Record

**The Honorable Michael C. Burgess**

- 1. The President recently called for a single, national standard for breach notification legislation. Do you have a response to the language he proposed? Please discuss.**

Answer: We appreciate the Administration's focus on a single national standard for breach notification legislation. Axiom does not believe that a new legislative proposal was necessary, since Congress has had the right basic provisions of a data breach notification bill under consideration for a number of years. However, we believe it is helpful for the Administration to weigh in supporting congressional action, as that may help build momentum for Congress's bill.

We do not believe that a 30-day notification requirement is in the public interest, and will discuss that in greater detail below.

- 2. Given the activity of States regulating data security in the last few years, is there a benefit for industry if Congress sets a national standard for reasonable data security? Would you support a preemptive reasonable data security standard? Please explain.**

Answer: Axiom would support a uniform federal data security standard. There is far more variance in State data security obligations than in breach notification obligations. A uniform federal standard likely would provide greater protection for individuals by instituting a standard of protection that is higher than may be the case in some organizations today. Furthermore, conflicting State data security obligations are more problematic than conflicting breach notification obligations. Companies don't develop security systems for each state. They develop them for the entire U.S. and often for the entire world.

A federal standard needs to be clear. Vague standards can facilitate unwarranted litigation. The standard also needs to be flexible enough to adapt as threats and capabilities adapt. We are comfortable providing the FTC with authority, which addresses the issue of flexibility. However, the FTC standard needs to be sufficiently concrete that companies do not have to worry about finding themselves on the wrong side of a regulator's expectations without fair notice.

- 3. How do you define preemption that would effectively eliminate the existing patchwork of State laws?**

Answer: My testimony included the following suggested formulation:

*No law, rule, regulation, requirement, standard, or other provision having the force and effect of law relating to data security or notification following a breach of data security may be imposed under State law or the law of a political subdivision of a State on a person subject to this Act.*

Subcommittee on Commerce, Manufacturing, and Trade  
What are the Elements of Sound Data Breach Legislation?

Response of:  
Ms. Jennifer Glasgow  
Global Privacy and Public Policy Executive  
Axiom Corporation

Other formulations also could be effective. Consumers need notice that is clear and meaningful; businesses need notice rules that are not unnecessarily inefficient and burdensome. Those two aims are both served by a single preemptive federal standard.

**4. How do you believe state common law should be treated in federal data security and breach notification legislation? Should it be preempted?**

Answer: Liability provides a disincentive to practices that cause harm, and compensation to those who are harmed. The regulation provided by the bill will make unlawful breach notification practices that could cause harm. As for compensating injured parties, injuries typically do not arise from notification or lack of notification, but from the breach itself. For these reasons, we believe Congress very reasonably could conclude that State common law with respect to breach notification should be preempted. Companies are better served if there is uniformity and predictability in the law. State common law provides neither.

**5. Please explain the issues that could develop in the marketplace if a federal data security and breach notification bill does not preempt State law.**

Answer: Congress would in essence be creating a 51<sup>st</sup> applicable law, which would only exacerbate the current problem. We would be better off without a federal law if it doesn't have preemption to establish a single standard. Congress would be making matters worse. If a federal law sits alongside a conflicting State law that is not preempted, consumers could receive more than one notice, which would be harmful by creating confusion. It would also be harmful because the added cost – again, in providing no benefit – ultimately will be borne by consumers and the economy.

**6. Do you support allowing State Attorneys General to enforce a federal data security and breach notification law if the law preemption current State law? Are there other factors that should be considered in extending this enforcement authority?**

Answer: While we prefer that federal law be enforced by federal entities, we also think it is important for sufficient resources to be available for enforcement. If the law is fully preemptive, we would not object to allowing State AGs to enforce the bill's requirements.

**7. There was testimony during the hearing that companies undertake investigations after a breach is discovered. Please explain the steps of a data breach investigation and what information companies learn during this process.**

Answer: Breaches can come from many places - hackers trying to break in to someone's system, other companies or countries stealing confidential data for commercial gain, and insiders leaking data intentionally or unintentionally. Furthermore, breaches can be discovered by the breached company themselves via their own detection systems, discovered by law enforcement in the investigation of

Subcommittee on Commerce, Manufacturing, and Trade  
What are the Elements of Sound Data Breach Legislation?

Response of:

Ms. Jennifer Glasgow  
Global Privacy and Public Policy Executive  
Axion Corporation

other unlawful conduct that may include the criminals' use of the stolen data, or discovered by investigative journalists. Also, a breach can be limited to one system or it can be distributed across many systems that may involve systems run by other entities or supported by vendors. Furthermore, it may take time to get subpoenas to investigate other parties, and law enforcement may need time to confiscate evidence before a breach becomes public and before the information is destroyed. Each of these factors can require a very different investigative, corrective, and restorative approach. Furthermore, investigations are not linear: you don't simply learn all at once about the problem and then fix it. A breached company may initially think the breach involved one system or one individual and investigate logs or other tracking records to determine the scope of the breach. Many times, this points to other systems, other individuals or other entities that also need to be investigated. Think of the process as iterative, often looping back on itself to necessitate more investigation after some fact is known.

8. **The dangers of over notification for consumers in the long term have been outlined by States, companies, and the Federal Trade Commission. Taking this issue into consideration, what should the risk trigger be for a company to notify individuals after a breach?**

Answer: It should be a reasonable risk of harm trigger. This is consistent with most of the existing state laws and the Gramm-Leach-Bliley Act. Furthermore, there is very little functional difference between terms such as "reasonable" or "significant" risk of harm, as we believe companies essentially would look at the facts in the same way when determining whether to notify.

9. **Is it practical to toll a notification deadline in federal data security and breach notification legislation to allow the breached entity time to secure and restore the breached system? Do any States take this approach in their breach notification statutes? I don't know State requirements, but I assume many do provide for such temporary suspension. If you don't toll, you risk notifying before you've fully learned what happened.**

Answer: It is not practical to have a firm deadline for breach notification. "As quickly as reasonably possible" is the idea; Congress needs to determine how to shape that into a legal standard. As outlined in my answer to question 7, the timeframe for discovering, securing and restoring a breached system is not predictable. If there is a notification deadline, some breaches will notify before all the facts are gathered and may have to do additional notifications once the investigation has further developed. If facts are discovered after an initial notice, it could result in the confusion of an additional notice to the same consumers. Most breaches are discovered months after they take place, or have been going on for months. We should not force an artificial deadline, but instead allow the investigation and restoration to proceed to completion.

Subcommittee on Commerce, Manufacturing, and Trade  
What are the Elements of Sound Data Breach Legislation?

Response of:  
Ms. Jennifer Glasgow  
Global Privacy and Public Policy Executive  
Acxiom Corporation

10. **What are cyber attackers typically looking for when they attempt to breach your members' networks? Do you know if the purpose is typically to embarrass the consumer or to steal his or her information for financial gain?**

Answer: From our experience and based on breaches reported in the press, the cyber attackers are typically looking for data for financial gain, either from ID theft or other scams that require knowledge of certain personal information in order to conduct the scam. Even in the scam situations the objective is financial gain.

**The Honorable Bobby Rush**

1. **It is my understanding that there are at least three categories of information that firms, such as Acxiom, provide information for. You discussed how consumers are able to correct errant information or opt out of marketing altogether. Are the changes consumers make to the marketing section carried throughout the other categories?**

Answer: Acxiom has three categories of information that we bring to the market. One is information for marketing purposes, another is information for risk mitigation and the third is telephone data for directory purposes. Each category is developed with the data specifically needed for that purpose and access, correction and opt-out rights appropriate for each. For marketing purposes, consumers can access, correct, delete elements or opt-out of all marketing uses via our website [www.aboutthedata.com](http://www.aboutthedata.com). We offer a complementary offline service for accessing and correcting the risk mitigation information because we do stronger authentication for this data that contains sensitive elements like SSN and DL#. For risk information we do not offer opt-out because we don't allow the bad buys to opt-out of the very systems designed to catch them. The final category, directories, contains names and phone numbers and is only compiled from public records and directory assistance. Consumers can opt-out of this, but we do not provide a correction feature.

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641  
March 4, 2015

Mr. Woodrow Hartzog  
Cumberland School of Law  
Samford University  
800 Lakeshore Drive  
Birmingham, AL 35229


Dear Mr. Hartzog,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, January 27, 2015 to testify at the hearing entitled "What are the Elements of Sound Data Breach Legislation?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, March 18, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at [Kirby.Howard@mail.house.gov](mailto:Kirby.Howard@mail.house.gov) and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,  
  
Michael C. Burgess  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade  
Attachment



**Woodrow Hartzog**  
**Associate Professor**  
**Samford University's Cumberland School of Law**  
**3-13-15**

Additional Questions for the Record

**The Honorable Michael C. Burgess**

1. The President recently called for a single, national standard for breach notification legislation. Do you have a response to the language he proposed? Please discuss.

*The version of the President's proposed language that I have seen has some commendable elements. It allows for a flexible definition of SPII to be modified by rulemaking, covers non-profit organizations, requires notice without unreasonable delay with a 30 day cap, empowers the FTC and provides a safe harbor when there is no reasonable risk of harm instead of a harm trigger. However, it is too preemptive of federal and state protections, improperly excludes paper records and other non-digital data, and has thin notice requirements, including no requirement to inform third parties like credit reporting databases under some circumstances and no requirement to list when the breach occurred. Sound data breach legislation should also include a nationwide requirement for businesses to provide reasonable data security.*

2. In many cases, a breach in data security is the result of criminal hacking. Do you support private causes of action for data breaches against the companies that were victims of a breach? Please explain your position on private causes of action taking into consideration the fact that private causes of action expose a company to liability when the real culprit is the intruder/criminal that hacked the company's system.

*I support private causes of action in instances where demonstrable harm resulted from unreasonable data security practices. Not every data breach should give rise to liability. However, consumers can suffer harm as a result of negligent data security practices, which is precisely what private causes of action are intended to remedy. Companies are victims of the hackers, but also sometimes culpable for failing to protect data entrusted to them by consumers.*

**The Honorable Tony Cárdenas**

1. Recently, I had an amendment included in the National Defense Authorization Act (NDAA) to help smaller defense subcontractors who may not have information technology departments prepare themselves for cyber-attacks. What aspects of data breach legislation take into account the differences between big and small businesses?

*A data security requirement using a reasonableness standard would presumably incorporate the differences between big and small businesses. A small business collecting only small amounts of personal information does not need to have the exact same data security as large corporations like Target and Microsoft. The FTC has said as much in its statement issued with its 50<sup>th</sup> data security settlement, saying, "a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it*

*holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."*

2. As the recent data breach attacks on Sony show, cybersecurity issues can quickly lead to the release of private and intimate information of many Americans and drastically harm a company's financial well-being. With even the largest of American companies at risk, what financial risks do we continue to run by not putting together a bipartisan solution that can be signed by the President?

*There are few issues more important to commerce and our national infrastructure than data security. While the FTC has admirably regulated data security for the past twenty years, it could benefit from more resources and specific rulemaking authority. Poor data security regulation not only runs the risk of financial loss from fraud, it also risks financial loss in the form of lost consumer confidence. People will be forced to withdraw from the marketplace if they cannot trust that their information will be protected.*

*However, it is important to emphasize that federal data breach legislation could do more harm than good if it weakens the existing hard-won state and federal protections. Companies already have obligations to keep data secure and notify users in case of a breach. These obligations are not dramatically different from each other and virtually all data security laws simply require a reasonable adherence to industry standards. While federal data breach legislation could provide more protection, there is no urgency to produce a weaker solution.*

3. Have consumers, whose buying habits, identities, and financial information are at risk, been notified of how much of their information is currently at risk?

*In a technical sense, consumers are notified when their data is breached and they are reminded daily by the media of how vulnerable companies are. But in practice, this only somewhat benefits consumers. Data security is opaque to consumers. Short of eternal vigilance, credit freezes and withdrawals from the marketplace, consumers are limited in the ways they can minimize the risk of personal disclosure in the modern age. This is why any federal solution should include data security requirements and breach notice requirements to third parties such as state attorneys general, credit reporting agencies, and the media.*