

DISCUSSION DRAFT OF H.R. _____, THE DATA
SECURITY AND BREACH NOTIFICATION ACT
OF 2015

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

MARCH 18, 2015

Serial No. 114-21



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

U.S. GOVERNMENT PUBLISHING OFFICE

22-433 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	1
Prepared statement	3
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement	4
Prepared statement	5
Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement	6
Prepared statement	7
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	9
Prepared statement	10

WITNESSES

Hon. Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission	11
Prepared statement	14
Answers to submitted questions	215
Clete D. Johnson, Chief Counsel for Cybersecurity, Federal Communications Commission	30
Prepared statement	32
Jon Leibowitz, Co-Chairman, 21st Century Privacy Coalition	59
Prepared statement	61
Answers to submitted questions ¹	217
Sara Cable, Assistant Attorney General, Commonwealth of Massachusetts	68
Prepared statement	70
Answers to submitted questions	218
Mallory B. Duncan, Senior Vice President and General Counsel, National Retail Federation	100
Prepared statement	102
Answers to submitted questions ¹	225
Laura Moy, Senior Policy Counsel, Open Technology Institute, New America ..	138
Prepared statement	140
Answers to submitted questions ²	226
Yael Weinman, Vice President for Global Privacy Policy and General Counsel, Information Technology Industrial Council	153
Prepared statement	155
Answers to submitted questions	227

SUBMITTED MATERIAL

Discussion Draft, H.R. _____, the Data Security and Breach Notification Act of 2015, ³ submitted by Mr. Burgess	
Letter of March 18, 2015, from Public Knowledge, et al., to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Pallone	183

¹ Mr. Leibowitz and Mr. Duncan did not answer submitted questions for the record by the time of printing.

² Ms. Moy's answers have been retained in committee files and also are available at <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf>.

³ The discussion draft has been retained in committee files and also is available at <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-20150318-SD003.pdf>.

IV

	Page
Letter of March 18, 2015, from Ellen Bloom, Senior Director, Federal Policy and Washington Office, et al., Consumers Union, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Pallone	186
Letter of March 17, 2015, from Jim Nussle, President and CEO, Credit Union National Association, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess	187
Letter of March 16, 2015, from Howard Fienberg, Director of Government Affairs, Marketing Research Association, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess	190
Letter of March 16, 2015, from Brad Thaler, Vice President of Legislative Affairs, National Association of Federal Credit Unions, to Mr. Upton, et al., submitted by Mr. Burgess	191
Letter of March 17, 2015, from Craig D. Spiegle, Executive Director and President, Online Trust Alliance, to Mr. Burgess and Ms. Schakowsky submitted by Mr. Burgess	194
Statement of National Association of Convenience Stores, March 18, 2015, submitted by Mr. Burgess	202
Statement of American Bankers Association, et al., March 18, 2015, submitted by Mr. Burgess	210
Answers to House Committee on Energy and Commerce questions submitted to the Secret Service, February 19, 2015, submitted by Mr. Burgess	213

**DISCUSSION DRAFT OF H.R. _____, THE DATA
SECURITY AND BREACH NOTIFICATION ACT
OF 2015**

WEDNESDAY, MARCH 18, 2015

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

The subcommittee met, pursuant to call, at 10:02 a.m., in room 2123 of the Rayburn House Office Building, Hon. Michael Burgess (chairman of the subcommittee) presiding.

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

Also present: Representative McNerney.

Staff present: Charlotte Baker, Deputy Communications Director; Leighton Brown, Press Assistant; Karen Christian, General Counsel; James Decker, Policy Coordinator, Commerce, Manufacturing, and Trade; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Howard Kirby, Legislative Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Olivia Trusty, Professional Staff, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Christine Brennan, Democratic Press Secretary; Jeff Carroll, Democratic Staff Director; David Goldman, Democratic Chief Counsel, Communications and Technology; Lisa Goldman, Democratic Counsel; Brendan Hennessey, Democratic Policy and Research Advisor; and Tim Robinson, Democratic Chief Counsel.

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

Mr. BURGESS. Chair will recognize himself for the purpose of a 5-minute opening statement. Again, welcome. Today's legislative hearing is the first concrete step for this subcommittee toward the goal of a single Federal standard on data security and breach notification. In January we heard testimony about the key elements of sound data security and breach notification. I am pleased that so many of the elements discussed at that hearing have been incorporated into the draft legislation.

I also know, and I am aware of, that we just had another data breach that was in the news. I hope that the committee looks at health care data. Health care data has its own set of policy issues, where, if sharing data is done properly, could have tremendous public benefits and save lives, but there is already law in this area under HIPAA, and taking on health care privacy data in this bill I feel would delay the consumer benefits that we can provide under this draft.

I am very encouraged by the bipartisan approach and commitment shown by my colleagues, vice chairman of the full committee Congresswoman Blackburn, and Congressman Welch, announcing this draft legislation. This subcommittee has a history of bipartisan cooperation with the work of Congressman Barton and Congressman Rush, that they have put a lot into this issue over the years. I am encouraged that this may be the year that we find the paths forward.

The issue of data breach has been before this subcommittee for a decade, and it is in reference to that that this is such important work. I would just acknowledge the work of previous subcommittee chairs on both sides of the dais who have worked in this space. Chairman Bono Mack is here with us in the audience this morning. I heard from former Chairman Terry yesterday on the eve of starting this hearing. And certainly Chairman Rush, when I was in the minority and on this subcommittee, I know put in a lot of work.

But all the while that we have been working, cybercriminals have continued their operations. They steal, they monetize an individual's personal information, all of that being done in the absence of any national data security requirement. Even today the great majority of States do not have a data security requirement. Ten years in, we do have greater insight into what cybercriminals are doing, and the impact of their activities. Conservative estimates put cybercrime cost to the consumers at \$100 billion annually, and cybercrime is estimated to cost the United States economy over a half million jobs each year.

The Secret Service tells us that data breaches are primarily monetized through financial fraud. On average, a third of data breach notification recipients became the victims of identity fraud in 2013, compared with a quarter in 2012, clearly increasing. On a more personal level, individuals are hit twice when there is a data breach. First they need to understand which of their accounts they need to reset, if they need new bank cards, or if they need to freeze their credit report. Luckily, there are many laws to help navigate the process.

Second, the cost across the ecosystem is \$100 billion annually, and that is eventually passed on to the consumer in the form of higher fees and prices. The existing patchwork of State laws on data security and breach notification do not seem to have been effective. The noted security blogger Brian Krebs posted an article this week about the new criminal tools to steal customers' payment information, and he ended it with a simple question, are online merchants ready for the coming e-commerce fraud wave? The draft legislation before us this morning addresses this question with both a security requirement for personal information that leads to iden-

tity theft and payment fraud, and a breach notification for consumers so consumers can protect themselves.

Some will complain about what is not in the bill. If we actually want to pass legislation, it will be impossible to proof it against what can happen in the future. We cannot shade into areas such as privacy. This administration, and our minority colleagues, over the past 6 years have worked on this and still can't agree on how to address privacy, and I just want to be very clear on that topic. While we don't tackle privacy in this legislation, we don't preempt it either. This bill is focused on unauthorized access that leads to identity theft and financial fraud. It has nothing to do with permitted access, or when that permission can be given, or what data can be collected. I will also say that Congress must continue to address privacy of all kinds, but not at the price of delaying consumer protections for data security and breach notification.

Another complaint will be around moving the telecommunications, cable, and satellite providers from the Federal Communications Commission to the Federal Trade Commission. I look forward to hearing which agency has been more active—the more active consumer watchdog regarding data security and breach notification in the last 10 years.

I certainly do look forward to continuing the bipartisan good faith negotiations with all interested stakeholders. Negotiation remains open and ongoing, and, of course, the doors of the subcommittee are always open.

[The prepared statement of Mr. Burgess follows:]

PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

Today's legislative hearing is the first concrete step for this subcommittee toward the goal of a single Federal standard on data security and breach notification.

In January, we heard testimony about the key elements of sound data security and breach notification legislation. I am pleased to see so many of the elements discussed at that hearing incorporated into the draft legislation.

I know we just had another healthcare data breach. And I hope that the committee looks at healthcare data. Healthcare data has its own set of policy issues—where sharing data if done properly—could have tremendous public benefits and save lives. But there is law in this area—HIPPA—and taking on healthcare privacy and data in this bill would delay the consumer benefits that we can provide under this draft.

I am very encouraged by the bipartisan approach and commitment shown by my colleagues, vice chairman of the full committee Congresswoman Blackburn and Congressman Welch announcing this draft legislation. This subcommittee has a history of bipartisan cooperation with the work Congressman Barton and Congressman Rush have also put into this issue over the years. I am encouraged that this is the year we can find a path forward.

The issue of data breach has been before this subcommittee for many years and all the while, cybercriminals continued their operations to steal and monetize individuals' personal information. All in the absence of any national data security requirement. Even today, the great majority of States do not have a data security requirement.

Ten years in—we do have greater insight into what cybercriminals are doing and on their impact. Conservative estimates put cybercrime costs to consumers at \$100 billion annually. And cybercrime is estimated to cost the U.S. economy 508,000 jobs each year.

The Secret Service tells us that data breaches are primarily monetized through financial fraud. On average $\frac{1}{3}$ of data breach notification recipients became victims of identity fraud in 2013, compared with $\frac{1}{4}$ in 2012.

On a more personal level, individuals are hit twice when there is a data breach. First, they need to understand which of their accounts they need to reset, if they

need new bank cards, or if they need to place a freeze on their credit report. Luckily, there are many laws to help navigate that process.

Second, the costs across the ecosystem, that \$100 billion annually, are eventually passed to the consumer in the form of higher fees and prices.

The existing patchwork of State laws on data security and breach notification have not been effective.

The noted security blogger, Brian Krebs, posted an article this week about new criminal tools to steal customers' payment information that ended with a simple question: "Are online merchants ready for the coming e-commerce fraud wave?"

The draft legislation addresses this question with both the security requirement for personal information that leads to identity theft and payment fraud, and the breach notification for consumers so that they can protect themselves.

Some folks will complain about what is not in the bill. If we want to actually pass legislation we cannot future proof this bill. We cannot shade into areas such as privacy. This administration and our minority colleagues have had 6 years, and they still can't agree on how to address privacy.

On the topic of privacy—let me be very clear—while we don't tackle privacy we don't preempt privacy either. This bill is focused on unauthorized access that leads to identity theft and financial fraud. It has nothing to do with permitted access, or when that permission can be given, or what data can be collected. I will also say that Congress must continue to address privacy of all kinds, but not at the price of delaying consumer protections for data security and breach notification.

Another complaint will be around moving telecommunications, cable, and satellite providers from the Federal Communications Commission to the Federal Trade Commission. I look forward to hearing which agency has been the more active consumer watchdog regarding data security and breach notification in the last 10 years.

I look forward to continuing the bipartisan and good faith negotiations with all interested stakeholders. Negotiations remain ongoing, and our doors are always open.

Mr. BURGESS. With that, I would like to recognize the ranking member of the subcommittee, Ms. Schakowsky, 5 minutes for 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. I appreciate the hearing today on the draft legislation released last week, and—by Mr. Welch and Ms. Blackburn to require data breach security and reporting. I do appreciate my colleagues' efforts on this legislation, and I agree that there are some positive elements, FTC penalty authority and a data security provision among them.

That said, however, this bill does need significant amendments to achieve the goal of both simplifying compliance for business, and enhancing protections for consumers. I don't believe that goal is out of reach. I don't think that it expands the time that it will take. Maybe by just a bit, but the draft proposal would—has these problems, in my view. It would prevent States from enforcing their own laws related to data security and breach notification. It prevents all private rights of action on data breach and notification. As currently drafted, it would override all common law, including tort and contract law, as they apply to data. Those provisions would leave consumers with fewer protections than they currently have.

This proposal also weakens existing consumer protections under the Communications Act for customers of telecommunications, satellite, and cable companies. And while I believe the FTC can, and should, be empowered to play a stronger role in protecting consumers' data, I don't believe that should come at a cost of eliminating existing FCC protections. The bill would also only require

consumers to be notified of a breach if it is determined that a breach has, or will, likely lead to financial harm. That would only occur after the companies regulated under this bill have concluded investigations of breaches to determine the risk of financial harm to each of their customers or users, a process that could take months.

There are many types of harm that go beyond simply financial ones. For example, a data breach that revealed private communication might not have any measurable financial impact, but could cause embarrassment, or even danger. The types of personal information covered by this bill are far too limited. The bill doesn't cover over the counter drug purchases, or other health information not covered by HIPAA. By contrast, the data laws in Texas and Florida protect those types of information. The bill does not cover metadata, which can be used to acquire sensitive personal information. The bill also does not provide FTC rulemaking authority for defining personal information. This is a major weakness when we have seen the nature of personal information change significantly over time. For example, when the House passed the Data Act in 2009, it did not include geolocation information as part of personal information. Today I think we could all agree that geolocation information should be protected, and that is why we need legislation that allows the FTC to adapt as the nature of personal information continues to evolve. Of course we can't anticipate everything, but we could create some flexibility.

In closing, this bill is very broad, in terms of preemption of State and other Federal laws, and narrow in terms of definitions of harm and personal information. I believe the bill should be narrow where it is now broad, and broad where it is now narrow. I look forward to hearing from our witnesses about their perspectives on this bill, and to moving forward with a strong bill that adequately protects consumers.

[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 draft legislation released last week by Mrs. Blackburn and Mr. Welch to require data breach security and reporting.

I appreciate my colleagues' effort on this legislation, and I believe it has some positive elements—FTC penalty authority and a data security provision among them.

That being said, this bill needs significant amendment to achieve the goal of both simplifying compliance for businesses and enhancing protections for consumers.

The draft proposal would prevent States from enforcing their own laws related to data security and breach notification. It prevents all private rights of action on data breach and notification. As currently drafted, it would override all common law—including tort and contract law—as they apply to data. Those provisions would leave consumers with fewer protections than they currently have.

This proposal also weakens existing consumer protections under the Communications Act for customers of telecommunications, satellite, and cable companies. While I believe the FTC can and should be empowered to play a stronger role in protecting consumers' data, I don't believe that should come at a cost of eliminating existing FCC protections.

The bill would also only require consumers to be notified of a breach if it is determined that a breach has or will likely lead to financial harm. That would only occur after the companies regulated under this bill have concluded investigations of breaches to determine the risks of financial harm to each of their customers or users—a process that could take months.

There are many types of harm that go beyond simply financial ones. For example, a data breach that revealed private communications might not have any measurable financial impact, but could cause embarrassment or shame.

The types of personal information covered by this bill are far too limited. The bill doesn't cover over-the-counter drug purchases or other health information not covered by HIPAA. By contrast, the data laws in Texas and Florida protect those types of information. The bill also does not cover metadata, which can be used to acquire sensitive personal information.

The bill also does not provide FTC rulemaking authority for defining personal information. That is a major weakness when we've seen the nature of personal information change significantly over time. For example, when the House passed the DATA Act in 2009, it did not include geolocation information as part of personal information. Today, I think we could all agree that geolocation information should be protected. That is why we need legislation that allows the FTC to adapt as the nature of personal information continues to evolve.

In closing, this bill is very broad in terms of preemption of State and other Federal laws and narrow in terms of definitions of harm and personal information. I believe the bill should be narrow where it is now broad, and broad where it is now narrow. I look forward to hearing from our witnesses about their perspectives on this bill and to moving forward with a strong bill that adequately protects consumers. With that, I yield the remainder of my time to Mr. Kennedy.

Ms. SCHAKOWSKY. With that, I yield the remainder of my time to Mr. Kennedy.

Mr. KENNEDY. Thank you very much to my colleague, and thank you for—my colleagues on both sides of the aisle for their efforts in pulling this bill together. It is always nice to see a Bay Stater here to testify before the committee, so I just wanted to give a warm welcome to Sara Cable, Massachusetts Assistant Attorney General with the Consumer Protection Division. Ms. Cable investigates and prosecutes violations of the Massachusetts Consumer Protections Act and the Massachusetts data notification laws and data security regulations. I have no doubt that the work that Ms. Cable does in enforcing Massachusetts data breach laws has protected many across the Commonwealth, and I truly appreciate her being willing to be here today and take some time to share her thoughts and expertise with us about an incredibly important issue.

And with that, Ms. Schakowsky, I will yield back. Thank you.

Mr. BURGESS. Chair thanks the gentlelady. Gentlelady yields back. The Chair now recognizes the chairman of the full committee, Mr. Upton, 5 minutes for an opening statement.

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

Mr. UPTON. Well, thank you. We are at a critical point for consumer protection in the U.S. Our interconnected economy, with many great benefits, also poses new threats from thieves, new challenges to information security, that is for sure. And as the Internet weaves itself into the DNA of appliances, cars, clothing, the threats of exploitation multiply, but the most serious underlying criminal purpose remains the same, to steal and monetize personal information, and it has to be stopped.

As data breaches have evolved, the one constant is that identity theft and payment card fraud are the crimes that pay the criminals. According to the Bureau of Justice Statistics, personal identity theft costs our economy nearly \$25 billion in '12, making it the largest threat to personal property today. There is not a single

member of this committee who doesn't represent someone who has suffered either identity theft or payment fraud.

This bipartisan draft legislation that we consider today establishes a reasonable national security standard, with flexibility to adapt to changing security technology. The FTC and the State Attorneys General will be policing companies to hold them accountable for protecting consumers. The draft also focuses on the personal information that criminals have targeted, the cyber gold that attracts today's cybersafecrackers. I want to thank my colleagues Blackburn and Welch for bringing us a big step closer to a bipartisan solution. Other members of the committee, including Mr. Barton and Rush, have also rolled up their legislative sleeves over the years. And I want to thank Chairman Burgess for making this issue a very top priority on this subcommittee.

I also commend the narrow approach. By targeting the most sought after personal information in the areas lacking current Federal protections, this bill avoids controversial issues that have derailed past efforts. Our goal is to create clear requirements to secure personal information from, and notify consumers in cases of unauthorized access. The goal is not to broadly regulate the use of data.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

We are at a critical point for consumer protection in the United States. Our interconnected economy, with many great benefits, also poses new threats from thieves and new challenges to information security. As the Internet weaves itself into the DNA of appliances, cars, and clothing, the threats for exploitation multiply, but the most serious underlying criminal purpose remains the same: to steal and monetize personal information.

As data breaches have evolved, the one constant is that identity theft and payment card fraud are the crimes that pay the criminals. According to the Bureau of Justice Statistics, personal identity theft cost our economy nearly 25 billion dollars in 2012, making it the biggest threat to personal property today. There is not a single member of this committee who doesn't represent someone who has suffered from either identity theft or payment fraud. I know in southwest Michigan it's a real concern.

The bipartisan draft legislation we consider today establishes a reasonable national security standard with the flexibility to adapt to changing security technology. The FTC and the State AGs will be policing companies to hold them accountable for protecting consumers. The draft also focuses on the personal information that criminals have targeted—the cyber gold that attracts today's cybersafecrackers.

I would like to thank Representatives Blackburn and Welch for bringing us a big step closer to a bipartisan solution. Other members of the committee, including Mr. Barton and Mr. Rush, have also rolled up their legislative sleeves over the years on this. And I thank Chairman Burgess for making this issue the top priority of the subcommittee.

I also commend the narrow approach—by targeting the most sought-after personal information and the areas lacking current Federal protections, this bill avoids controversial issues that have derailed past efforts. Our goal is to create clear requirements to secure personal information from—and notify consumers in cases of—unauthorized access; the goal is not to broadly regulate the use of data.

Some have argued that our legislation should be in addition to State laws. But the truth is, the State approach has not addressed the problem and does not adequately protect all consumers. We need a single, Federal set of rules. Companies and enforcers alike should focus on ensuring everyone is living up to that standard.

Mr. UPTON. I yield the balance of my time to Ms. Blackburn.

Mrs. BLACKBURN. I thank the chairman for yielding, and I also want to recognize the previous chairman of this committee, Ms. Bono, with us today, who have worked so diligently on this issue through the years. I appreciate the guidance and the leadership there. I also want to commend Mr. Welch, who has been co-chairman of the Privacy Working Group, and the chairman for allowing the Privacy Working Group a full 2 years to dig into this issue, and to see where we could find agreement. And that is the basis of the draft legislation that we have before us today.

The reason it is important that we do something now is because 2014 was dubbed the Year of the Breach. Think about the number of breaches that were out there. Our constituents have begun to see this firsthand. It has affected someone in nearly every family. And what they are saying is the issue is getting out of control, and we need to take steps to put the guidance in place so that individuals will know they have the tools that are necessary to protect their data, and, as I say, their virtual you, their presence online.

And I appreciate Mr. Welch and the work he and the Privacy Working Group did to help us come to this point, and I yield the balance of my time to the gentleman from Vermont.

Mr. WELCH. Congress hasn't been doing its job. We need to pass legislation that is going to deal with this incredible problem. You know, since 2005 a billion consumer records have been hacked into. The current status right now, we have got States trying to do something. Forty-seven different State laws on notice, 12 State laws on data security, but we don't have any national standard, and we don't have any legislative authority for the FTC, or really, for that matter, the FCC to do much, so we have to act and let there be a cop on the beat to protect people.

What this bill does—and this is a discussion draft, and I appreciate the back and forth, but we are going to have to have Mr. Pallone and Ms. Schakowsky very much involved as we go forward. What this does, it gives—it is a narrow bill. In my view, that is smart, because we have got to solve a problem. It gives the FTC explicit statutory authority, and that is being litigated in the Wyndham Hotels case. They can impose robust civil penalties. That is good. It does preempt States, but it doesn't limit the States with respect to the States, but it doesn't limit States on privacy issues, where they want to continue having legislative interaction.

This bill does not do some things that would be controversial that are debatable, but should not be part of this, because it will weigh it down. It is not a privacy bill. The States have continued authority in that space. It is not a bill about net neutrality. Big debate on this panel about the recent order. I happen to support it. Many of my colleagues don't. This bill is not about that. This bill is not about the common law right of action under tort law. Again, a debate here, but not something that we want to weigh this bill down.

Mr. Chairman, I appreciate the focus, the narrow focus on this. I appreciate Jan Schakowsky, the opportunity you gave me to work with the Privacy Group, and I implore all of my colleagues here to keep this going. We had good input from all of the affected parties, the FTC, the FCC consumer groups. We have got to get something

done, and we have got an opportunity in this committee to do it. I hope we can all be part of that.

I yield back.

Mr. BURGESS. Chair thanks the gentleman, gentleman yields back. The Chair recognizes the ranking member of the full committee, Mr. Pallone, 5 minutes for an opening statement.

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

Mr. PALLONE. Thank you, Chairman Burgess. Today we are discussing a draft data security and breach notification bill released recently by the majority. Data breaches are a plague on consumers, businesses, and our economy as a whole. Reducing the incidences of breaches, and the adverse effects from them, has rightfully been at the top of our agenda since 2005, yet it also has proven to be a complicated issue, without an easy legislative solution. I appreciate the efforts being taken to address the data breach problem, and I appreciate the difficulty of writing legislation that effectively protects consumers and lessens the burdens on the businesses that are victims of criminal breaches.

And while the sincerity of the efforts are not questioned, I do question the merits of the bill before us today. The bill simply does not strike the right balance. There are clearly benefits to creating a unified system for breach notification, but we must be careful that a Federal law ensures that protections for consumers are not being weakened. Many of the 51 State and territorial breach notification laws provide greater protections for consumers whose personal information is at risk as a result of data breach. For example, at least seven States and DC do not require a harm analysis before providing notice to consumers. At least 17 State laws also include a private cause of action. At least nine States' laws cover health information.

In contrast, the draft under discussion today preempts stronger State and Federal laws, requires a financial harm analysis, preempts State private rights of action, and does not cover health or location information. Data breach notification is only part of the solution. The other crucial piece of any legislation should be baseline data security to help prevent breaches before consumers' personal information is put at risk. The draft before us eliminates State data security laws and replaces them with an unclear standard that will surely be litigated and left to judicial interpretation.

As I said at a hearing this past January, I want to be supportive of sound data security and breach notification legislation, but to get there we must ask the right question. The question is not whether any one Federal agency would be better off. The question must always be whether legislation puts consumers in a better place than they are today. And, unfortunately, the draft before us today does not put consumers in a better place, in my opinion.

So before I close, I have to raise a process issue. We received the draft bill last Thursday evening. The 114th Congress seems to have halted a long tradition of sharing text with all members of the subcommittee at least a full week prior to a legislative hearing, and this is not the first time this has happened this year in the Energy

and Commerce Committee, as we saw with our Communications Subcommittee. I suspect it is not going to be the last.

Also, I know this may sound, you know, a little picky, but I have to take issue with Chairman Burgess' opening remarks and repeat my longstanding belief that having some Democratic support does not make a measure bipartisan. I think that Chairman Upton used better language when he said maybe it is a step closer to being bipartisan. And I appreciate what Mr. Welch said, which is that—he mentioned having the support of myself and Ms. Schakowsky on a bill. I would like to see this bill improved before it moves further through the legislative process so that all members of the committee can support it, and it can be a truly bipartisan legislative product, which it is not at this time.

I have some time left. Did you want additional time? All right. Yvette, or—everybody is OK? All right. Thank you, Mr. Chairman. I will yield back the balance of my time.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you Mr. Chairman. Today we are discussing a draft data security and breach notification bill released recently by the majority.

Data breaches are a plague on consumers, businesses, and our economy as a whole. Reducing the incidences of breaches and the adverse effects from them has rightfully been at the top of our agenda since 2005. Yet, it also has proven to be a complicated issue without an easy legislative solution.

I appreciate the efforts being taken to address the data breach problem, and I appreciate the difficulty of writing legislation that effectively protects consumers and lessens the burdens on the businesses that are the victims of criminal breaches.

While the sincerity of the efforts are not questioned, I do question the merits of the bill before us today. This bill simply does not strike the right balance.

There are clearly benefits to creating a unified system for breach notification. But we must be careful that a Federal law ensures that protections for consumers are not weakened.

Many of the 51 State and territorial breach notification laws provide greater protections for consumers whose personal information is at risk as a result of a data breach. For example, at least seven States and the District of Columbia do not require a harm analysis before providing notice to consumers. At least 17 States' laws also include a private cause of action. At least nine States' laws cover health information.

In contrast, the draft under discussion today preempts stronger State and Federal laws, requires a financial harm analysis, preempts State private rights of action, and does not cover health or location information.

Data breach notification is only part of the solution. The other crucial piece of any legislation should be baseline data security to help prevent breaches before consumers' personal information is put at risk. The draft before us eliminates State data security laws and replaces them with an unclear standard that will surely be litigated and left to judicial interpretation.

As I said at a hearing this past January, I want to be supportive of sound data security and breach notification legislation. But to get there, we must ask the right question. The question is not whether any one Federal agency would be better off. The question must always be whether legislation puts consumers in a better place than they are today. Unfortunately, the draft before us today does not put consumers in a better place.

Before I close, I must raise process issues. We received the draft bill last Thursday evening. The 114th Congress seems to have halted a long tradition of sharing text with all members of the subcommittee at least a full week prior to a legislative hearing. This is not the first time this has happened this year in Energy and Commerce, and as we saw with our Communications Subcommittee, I suspect it won't be the last. Also, I must take issue with Chairman Burgess' opening remarks and repeat my longstanding belief that having token Democratic support does not make a measure bipartisan.

In closing, I hope we can work together to improve this bill before it moves further through the legislative process so that all members of the committee can support it and it can be a truly bipartisan legislative product.

Mr. BURGESS. Gentleman yields back. His observation is noted. I do want to welcome all of our witnesses, and thank you for agreeing to testify before the subcommittee today. Today's hearing will consist of two panels. Each panel of witnesses will have the opportunity to give an opening statement, followed by a round of questions from our members. Once we conclude with questions for the first panel, we will take a brief break to set up for the second panel.

For our first panel today, we have the following witnesses: Ms. Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission; and Mr. Clete Johnson, the Chief Counsel for Cybersecurity, Public Safety, and Homeland Security at the Federal Communications Commission. Thank you for your participation today. Ms. Rich, you are recognized for 5 minutes for the purpose of an opening statement.

STATEMENTS OF HON. JESSICA RICH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; AND CLETE D. JOHNSON, CHIEF COUNSEL FOR CYBERSECURITY, FEDERAL COMMUNICATIONS COMMISSION

STATEMENT OF JESSICA RICH

Ms. RICH. Dr. Burgess, Ranking Member Schakowsky, and members of the subcommittee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony on the subcommittee's data security legislation.

Reports of data breaches affecting millions of Americans fill the headlines. These breaches involved not just financial data, but other types of sensitive data, such as medical information, account credentials, and even the contents of private emails. These events serve as a constant reminder that consumers' data is at risk. Hackers and others seek to exploit vulnerabilities, obtain consumers' sensitive information, and misuse it in ways that can cause serious harms to consumers and businesses. Indeed, identity theft continues to be the FTC's number one source of consumer complaints, and data shows that over 16 million consumers were victimized in 2012 alone.

Every year, new incidents are reported that re-ignite concern about data security, as well as debate about the best way to provide it. Companies must implement strong data security measures to minimize consumers' risk of fraud, identity theft, and other substantial harm. Poor data security practices also creates risks for businesses. Data breaches can harm a company's financial interest and reputation, and also result in the loss of consumer trust. We need strong legislation now for consumers and the health of the commercial marketplace.

As the Nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. The FTC would like to thank the subcommittee for proposing enactment of Federal data security and

breach notification law, which the Commission has long supported on a bipartisan basis.

The Commission supports a number of elements in the proposed legislation which will give us additional tools to deter unlawful conduct. First, the bill includes a provision requiring companies to implement reasonable data security standards in addition to breach notification, both of which are essential to protect consumers. Second, the legislation gives the FTC jurisdiction to bring cases against non-profits and common carriers. Third, the bill provides for civil penalties, which are important to ensure adequate deterrents.

However, other aspects of the draft legislation don't provide the strong protections needed to combat data breaches, identity theft, and other substantial consumer harms. First, the bill does not cover precise geolocation and health data, even though misuse of this and other information can cause real harm to consumers, and even though a lot of health information is not, in fact, covered by HIPAA. For example, we brought a case last year against a medical transcription company whose lax security practice resulted in psychiatrists' notes about individual patients being made available on the Internet, available through simple Google searches. Given the definition of personal information in this bill, we would not be able to rely on the legislation to bring that case and seek civil penalties.

In addition to companies being careless with consumer information, hackers have incentives to obtain this data, even when it is not financial. For example, in some of our recent investigations, we have seen bad actors hack into company systems to steal consumers' information so they can extract payments from the companies for its return. A number of State laws currently protect consumers' health information, but those protections would be preempted under the bill.

Second, the Commission believes that data security protection should apply to devices that collect data, such as some Internet-enabled devices. Breaches involving these devices raise broader safety concerns, even if no data is stolen. For example, if a pacemaker isn't properly secured, a breach could result in serious harm to the person using it. Similarly, a malicious criminal who hacks into a car's network could disable its brakes, and other safety features.

Third, the FTC continues to believe that data security and breach legislation should include rulemaking authority under the Administrative Procedures Act. Rulemaking would allow the Commission to ensure that, as technology changes, and the risks from the use of certain types of information evolve, the law keeps pace, and consumers are adequately protected.

Finally, the FTC believes that any trigger for providing notification should be sufficiently balanced so that consumers can protect themselves when their data is at risk without experiencing over-notification. Accordingly, we support an approach that requires notice, unless a company can establish that there is no reasonable likelihood of economic, physical, or other substantial harm.

Thank you very much for this opportunity to provide the Commission's views. The FTC remains committed to promoting reasonable security for consumer data, and stands ready to work with the

subcommittee as it develops and considers legislation to protect consumers' sensitive information.

[The prepared statement of Ms. Rich follows:]

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

on

Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

March 18, 2014

I. INTRODUCTION

Doctor Burgess, Ranking Member Schakowsky, and members of the Subcommittee, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s testimony on data security legislation.

In the last year, headlines have been filled with reports of data breaches impacting millions of Americans.² These events serve as a constant reminder that consumers’ data is at risk. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers’ sensitive information, and potentially misuse it in ways that can cause serious harms to consumers and businesses. But data breaches are not a new phenomenon. We have been hearing about them for over a decade. Every year, new incidents are reported that reignite concern about data security, as well as debate about the best way to provide it.

The need for companies to implement strong data security measures is clear: if sensitive information falls into the wrong hands, the results can be devastating. Consumers face the risk of fraud, identity theft, and other harm. As one example, the Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012.³ Apart from the significant impact on individual consumers’

¹ This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

² See Elizabeth A. Harris & Nicole Perloth, *For Target, the Breach Numbers Grow*, N.Y. Times, Jan. 10, 2014, available at <http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html> (discussing recently-announced breaches involving payment card information by Target and Neiman Marcus); Nicole Perloth, *Michaels Stores Is Investigating Data Breach*, N.Y. Times, Jan. 25, 2014, available at <http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html> (discussing Michaels Stores’ announcement of potential security breach involving payment card information).

³ See Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at

lives, there are business and commercial ramifications – data breaches can harm a business’s financial interests and reputation and also result in the loss of consumer confidence in the marketplace. With unrelenting reports of data breaches, and with a significant number of Americans suffering from identity theft, the time for strong legislation is now.

As the nation’s consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. The Commission has undertaken substantial efforts for over a decade to promote data security in the private sector through civil law enforcement, business outreach and consumer education, policy initiatives, and recommendations to Congress to enact legislation in this area. This testimony provides an overview of the Commission’s efforts and its views on the subcommittee’s draft data security legislation.

II. THE COMMISSION’S DATA SECURITY PROGRAM

A. Law Enforcement

The Commission enforces several statutes and rules that impose data security requirements on companies. The Commission’s Safeguards Rule, which implements the Gramm-Leach-Bliley Act (“GLB Act”), for example, sets forth data security requirements for non-bank financial institutions.⁴ The Fair Credit Reporting Act (“FCRA”) requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,⁵ and imposes safe disposal obligations on entities that maintain consumer report information.⁶ The

<http://www.bjs.gov/content/pub/pdf/vit12.pdf>.

⁴ 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

⁵ 15 U.S.C. § 1681e.

⁶ *Id.* at § 1681w. The FTC’s implementing rule is at 16 C.F.R. Part 682.

Children's Online Privacy Protection Act ("COPPA") requires reasonable security for children's information collected online.⁷ In addition, the Commission enforces the FTC Act's prohibition against unfair or deceptive acts or practices in cases where the Commission has reason to believe that a business made false or misleading claims about its data security procedures, or failed to employ reasonable security measures and, as a result, causes or is likely to cause substantial consumer injury.⁸

Since 2001, the Commission has used its deception and unfairness authority under these laws to take enforcement action and obtain settlements in more than 50 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information.⁹ In each of these cases, the practices at issue were not merely isolated mistakes. Instead, the Commission examined the company's practices as a whole and challenged alleged data security failures that were multiple and systemic. And through these actions and orders, the Commission has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.

For example, the FTC's case against TRENDnet, Inc. involved a video camera designed

⁷ 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

⁸ 15 U.S.C. § 45(a). If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5. Further, if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.

⁹ *See generally* http://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249.

to allow consumers to monitor their homes remotely.¹⁰ The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were “secure,” they had faulty software that left them open to online viewing, and in some instances listening, by anyone with a camera’s Internet address. According to the Commission’s complaint, this resulted in hackers posting 700 consumers’ live video feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with two years of free technical support.

The FTC also entered into settlements with Credit Karma, Inc.¹¹ and Fandango, LLC¹² to resolve allegations that the companies misrepresented the security of their mobile apps. Credit Karma’s mobile app allows consumers to monitor and access their credit scores, credit reports, and other credit report and financial data, and has been downloaded over one million times. Fandango’s mobile app allows consumers to purchase movie tickets and has over 18.5 million downloads. According to the complaints, despite claims that the companies provided reasonable security to consumers’ data, Credit Karma and Fandango did not securely transmit consumers’ sensitive personal information through their mobile apps. In particular, the apps failed to authenticate and secure the connections used to transmit this data, and left consumers’ information vulnerable to exposure – including Social Security numbers, birthdates, and credit

¹⁰ *TRENDnet, Inc.*, No. C-4426 (F.T.C. Jan. 16, 2014) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>.

¹¹ *Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc>.

¹² *Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc>.

report information in the Credit Karma app, and credit card information in the Fandango app. The Commission's settlements prohibit Credit Karma and Fandango from making misrepresentations about privacy and security, and require the companies to implement comprehensive information security programs and undergo independent audits for the next 20 years.

The FTC also has spent significant resources litigating two data security matters, both of which are ongoing. The first is a case against Wyndham Hotels, in which the Commission filed a lawsuit in federal court alleging that the company failed to protect consumers' personal information.¹³ According to the FTC's complaint, Wyndham and its subsidiaries repeatedly failed to take reasonable and basic security measures, such as using complex user IDs and passwords and deploying firewalls between the hotels and the corporate network. In addition, Wyndham allegedly permitted improper software configurations that resulted in the storage of sensitive payment card information in clear readable text. These systemic failures exposed consumers' data to unauthorized access – in this instance, the company allegedly suffered three data breaches in less than two years. The complaint alleges that these failures, among others, resulted in fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' account information to an Internet domain address registered in Russia.

The second matter is in administrative litigation that the Commission will decide as an adjudicative body. Accordingly, the Commission cannot discuss the matter in detail while it remains in administrative adjudication.

¹³ *FTC v. Wyndham Worldwide Corp. et al.*, Civil No. 13-1887 (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss), available at <http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation>. An appeal of the district court's decision in this matter is pending in the Third Circuit. *FTC v. Wyndham Hotels & Resorts, LLC, et al.*, No. 14-3514.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security, such as by issuing reports and hosting workshops on emerging business practices and technologies affecting consumer data. For example, recently the FTC released a staff report about the Internet of Things (“IoT”), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people.¹⁴ The report found a wide range of security practices among manufacturers of these products. Among other things, the report recommends that companies developing IoT products should secure device functionality and implement reasonable security by, for example, conducting risk assessments, hiring and training appropriate personnel, and monitoring access controls.

Last year, the FTC hosted a three-part “Spring Privacy Series” to examine the privacy implications of new areas of technology that have garnered considerable attention for both their potential benefits and the possible privacy concerns they raise for consumers.¹⁵ The series focused on three areas: mobile device tracking in retail stores; the use of predictive scoring to help companies predict consumer behavior and shape how they market to particular consumers; and health apps that consumers increasingly use to manage and analyze their health data. At the seminar on health apps, panelists noted that many businesses operating in the consumer generated and controlled health information space might not be covered by the Health Insurance

¹⁴ FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), available at <http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Commissioner Ohlhausen issued a concurring statement. See http://www.ftc.gov/system/files/documents/public_statements/620691/150127iotmkostmt.pdf. Commissioner Wright dissented to the release of the report. See http://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwtmt.pdf.

¹⁵ See Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues*, Dec. 2, 2013, available at <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues>.

Portability and Accountability Act (“HIPAA”), and thus would not be subject to HIPAA’s data security protections. Participants also expressed concern that inadequate data security could result in unauthorized access to data, and cited the importance of building security into products and services, as well as the risks of failing to do so. Participants pointed to secure storage, encryption, and strong password protection as steps companies could take to secure consumers’ data.

C. Business Guidance and Consumer Education

The Commission also promotes better data security practices through business guidance and consumer education. On the business guidance front, the FTC widely disseminates a business guide on data security¹⁶ and has developed both an online tutorial¹⁷ and a recent blog post¹⁸ based on the guide. These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. The Commission also releases materials directed to a non-legal audience regarding basic data security issues for businesses.¹⁹ In addition, the FTC develops data security guidance for specific industries. For example, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps,²⁰ and

¹⁶ See *Protecting Personal Information: A Guide for Business*, available at <http://www.ftc.gov/tips-advice/business-center/protecting-personal-information-guide-business>.

¹⁷ See *Protecting Personal Information: A Guide for Business (Interactive Tutorial)*, available at <http://www.ftc.gov/news-events/audio-video/video/protecting-personal-information-guide-business-promotional-video>.

¹⁸ FTC Blog, *Time 2 Txt About Data Security Basics?*, Jan. 23, 2015, at <http://www.ftc.gov/news-events/blogs/business-blog/2015/01/time-2-txt-about-data-security-basics>.

¹⁹ See generally <http://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security>.

²⁰ *Mobile App Developers: Start with Security* (Feb. 2013), available at <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security>.

we also recently developed blogs to provide data security guidance for tax preparers²¹ and human resource professionals.²²

The FTC also creates business educational materials on specific topics – such as the risks associated with peer-to-peer (“P2P”) file-sharing programs and companies’ obligations to protect consumer and employee information from these risks.²³ Further, the FTC recently released guidance about ways to provide data security for IoT devices, which includes tips such as designing products with authentication in mind and protecting the interfaces between an IoT product and other devices or services.²⁴

The Commission also engages in outreach to consumers. The FTC sponsors OnGuard Online, a website designed to educate consumers about basic computer security.²⁵ OnGuard Online and its Spanish-language counterpart, Alerta en Línea,²⁶ average more than 2.2 million unique visits per year.

Identity theft has been the top consumer fraud complaint to the FTC for 13 consecutive years, and tax identity theft – which often begins by thieves obtaining Social Security numbers and other personal information from consumers in order to obtain their tax refund – has been an

²¹ See FTC Blog, *Tax ID Theft Awareness: Tips for Tax Preparers Bear (P)repeating*, Jan. 15, 2015, at <http://www.ftc.gov/news-events/blogs/business-blog/2015/01/tax-id-theft-awareness-tips-tax-preparers-bear-prepeating>.

²² See FTC Blog, *HR Professionals: Deter Tax ID Theft with an Open-Door (but Closed-Drawer) Policy*, Jan. 27, 2015, at <http://www.ftc.gov/news-events/blogs/business-blog/2015/01/hr-professionals-deter-tax-id-theft-open-door-closed-drawer>.

²³ See *Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), available at <http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business>.

²⁴ See *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), available at <http://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>.

²⁵ See <http://www.onguardonline.gov>.

²⁶ See <http://www.alertaenlinea.gov>.

increasing source of the Commission's identity theft complaints.²⁷ The Commission hosts IDTheft.gov, which provides consumers who may be victims of identity theft with important information and tools to protect themselves and assist in the recovery process.²⁸ We are in the midst of overhauling the website to better assist consumers.²⁹ And recently, the FTC hosted a series of webinars and Twitter chats as part of Tax Identity Theft Awareness Week.³⁰ The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.

III. THE SUBCOMMITTEE'S DATA SECURITY BILL

The Commission would like to offer a few comments on the discussion draft of the subcommittee's bill. The FTC would like to thank the subcommittee for developing and proposing enactment of a federal data security and breach notification law, which the Commission has long supported on a bipartisan basis. The Commission supports the goals of the subcommittee's data security bill to establish broadly applicable data security standards for companies and require them, in certain circumstances, to notify consumers in the event of a breach.

In prior testimony before Congress, the FTC has called for federal legislation that would (1) strengthen its existing authority governing data security standards for companies and (2)

²⁷ In 2012, tax identity theft accounted for more than 43% of the identity theft complaints, making it the largest category of identity theft complaints by a substantial margin. See Press Release, *FTC Releases Top 10 Complaint Categories for 2012* (Feb. 26, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/02/ftc-releases-top-10-complaint-categories-2012>.

²⁸ See <http://www.idtheft.gov>.

²⁹ In response to the President's Executive Order of October 17, 2014 on Improving the Security of Consumer Financial Transactions, the FTC is developing and implementing a plan to make the recovery process for identity theft victims quicker and less burdensome. By May 15, 2015, we will overhaul IDTheft.gov to provide streamlined information for identity theft victims and people whose information is stolen. In later phases, we will enhance the online victim assistance process to help people take steps to recover from identity theft more easily from their computer or mobile device.

³⁰ See generally <http://www.consumer.ftc.gov/features/feature-0029-tax-identity-theft-awareness-week>.

require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.³¹ It is critical that companies implement reasonable security measures in order to prevent data breaches and protect consumers from identity theft and other harms. And when breaches do occur, notifying consumers will help them protect themselves from any harm likely to be caused by the misuse of their data. For example, in the case of a breach of Social Security numbers, notifying consumers will enable them to request that fraud alerts or security freezes be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. Although most states have breach notification laws in place, having a strong and consistent national requirement could simplify compliance by businesses while ensuring that all consumers are protected.

The Commission supports a number of elements in the proposed legislation. First, the bill includes a provision requiring that companies implement reasonable data security standards, in addition to a breach notification requirement. The Commission believes that both breach notification and data security standards are essential to protect consumers. Second, the legislation gives the Commission jurisdiction to bring cases against common carriers and non-

³¹ See, e.g., Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf; Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), available at <http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), available at <http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf>.

profits. This would help ensure that whenever covered personal information is collected from consumers, entities that maintain such data – such as educational institutions – adequately protect it.³² Third, the Commission supports the provision that gives us the ability to seek civil penalties, which are an important tool to deter unlawful conduct. Under current laws, the Commission only has the authority to seek civil penalties for data security violations with regard to children’s online information under COPPA, or credit report information under the FCRA.³³ By expanding the Commission’s jurisdiction and giving it civil penalty authority, the bill will give us additional tools that we do not currently have.

Additionally, the bill covers important personal information – including Social Security numbers, username and password when used to obtain money or anything of value, and biometric data when used to obtain money or anything of value – regardless of whether it is associated with an individual’s name. Social Security numbers alone can be used to commit identity theft, even if not paired with a name and address, especially when such numbers belong to children without credit histories.³⁴ Similarly, both an account username and password, and biometric data such as a fingerprint, can be used to gain access to an account, including potentially an account that allows charges to be incurred, even if the thief does not have the name of the account holder.

However, other aspects of the draft legislation do not provide the strong protections that

³² A substantial number of reported breaches have involved non-profit universities and health systems. See Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities), available at <http://www.privacyrights.org/data-breach/new>.

³³ The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(l).

³⁴ See, e.g., ID Analytics, *The Long Con: An Analysis of Synthetic Identities* (Oct. 2014); FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft* (July 12, 2011), available at <http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft>.

are needed to combat data breaches, identity theft, and other substantial consumer harms.³⁵ First, the definition of personal information does not protect some of the information which is currently protected under state law. Second, the bill should address the entire data ecosystem, including Internet-enabled devices. Third, the bill does not provide the Commission with rulemaking authority under the Administrative Procedure Act (APA), which is necessary to ensure that the bill's goals can still be achieved in an evolving marketplace. Finally, the scope of the breach notification trigger should be expanded to cover other substantial harm.

While the Commission understands the importance of targeting concrete, substantial harms, and has sought to do so in its own enforcement efforts, we are concerned the draft bill does not strike the right balance.³⁶ For instance, the draft bill does not cover certain types of consumer information – such as precise geolocation and health data – even though misuse of this and other information can cause real harm, including economic harm, to consumers. Revelations of cancer treatment, for example, might cause an individual to lose a job or to receive calls from debt collectors. Furthermore, bad actors have an economic incentive to target reservoirs of valuable geolocation and health data for sale to debt collectors or private investigators. Indeed,

³⁵ Commissioner Wright supports the data security and breach notification legislation as drafted and believes that it strikes the right balance in protecting consumers from cognizable and articulable economic and financial harms. He disagrees with his colleagues to the extent that they recommend expanding the proposed legislation beyond its current economic and financial scope.

³⁶ For example, our Unfairness Statement notes that when evaluating whether a business practice is unfair, “the Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm... Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair.” FED. TRADE COMM’N., *Letter to Hon. Wendell H. Ford & Hon. John C. Danforth, Committee on Commerce, Science, and Transportation*, FTC Policy Statement on Unfairness (Dec. 17, 1980) (appended to *Int’l Harvester Co.*, 104 F.T.C. 949, 1070 (1984)). See also *GMR Transcription Services Inc.*, No. C-4482 (F.T.C. Aug. 21, 2014) (consent order) (alleging deception and unfairness violations in a case where sensitive private medical information was made publically available), available at <https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter>.

the Commission has seen instances where bad actors have hacked into company systems and stolen consumers' personal information in order to extract payments for its return. In addition, a breach revealing very personal and private details, such as the fact that an individual attends counseling for addiction, or a child walks back and forth from school at a particular time every day, can result in real economic and physical harms. Therefore, companies that collect precise geolocation information that can pinpoint a consumer's physical location, or information about an individual's physical or mental health condition, should have a duty to provide reasonable security for this data. Some of the state data security and data breach laws that would be preempted under the draft bill currently protect this information.³⁷

The Commission believes that data security requirements should apply to all key parts of the data ecosystem, including to devices that collect data, such as some Internet-enabled devices, as bad actors could target such devices to cause physical harm even if they do not steal any data. For example, the Commission's recent IoT report noted the security risks associated with interconnected devices such as pacemakers and automobiles. Security breach of such devices could lead to the compromise of personal information, but also raise broader safety concerns. Accordingly, general data security legislation should address risks to both personal information and device functionality.

The FTC also continues to believe that data security and breach notification legislation should include rulemaking authority under the APA. For example, a decade ago it would have been extremely difficult and expensive for a company to track an individual's precise geolocation. The privacy of such sensitive information was protected by the sheer impracticality

³⁷ See, e.g., Fla. Stat. § 501.171(g)(1)(a)(IV)-(V) (defining "personal information" to include medical and health insurance information); Tex. Bus. & Com. Code § 521.002(a)(2)(B) (defining "sensitive personal information" to include medical information).

of collecting it. Today the explosion of mobile devices has made such information readily available. Similar situations will no doubt arise as technology advances. Rulemaking authority would allow the Commission to ensure that even as technology changes and the risks from the use of certain types of information evolve, companies are required to appropriately protect such data. Such rulemaking authority would ensure the continuing vitality of the proposed law in light of the almost certain innovations in technology and business models, which may use different types of personal information than those currently enumerated but still raise the same risks of identity theft, economic loss or harm, financial fraud, or other substantial harm. APA rulemaking requires a notice and comment process, in which the Commission receives feedback from all stakeholders. It is also subject to judicial review under well-established standards in the APA. In other circumstances where Congress has given the Commission rulemaking authority under the APA, the agency has acted judiciously in accord with Congressional direction.³⁸

Finally, the FTC believes that any trigger for providing notification should be sufficiently balanced so that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive. Notification is crucial as it is the consumer who is best positioned to monitor and protect his/her interests in the event of a breach. Under the current draft of the bill, consumers are entitled to notice “[u]nless there is no reasonable risk that the breach has resulted in, or will result in, identity theft, economic loss or economic harm, or financial fraud.” The Commission is concerned that this standard will prevent consumers from receiving important breach

³⁸ For example, the Commission has issued the Telemarketing Sales Rule, 16 CFR Part 310, under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, as well as rules, 16 CFR Part 316, under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. § 7701 et seq.

notifications. The harm resulting from a breach may very well extend beyond economic or financial injury. For example, as discussed above, the breach of location data can reveal very sensitive information, such as whether an individual attends counseling, or the daily routines of a child. In the wrong hands, such information can result in economic and physical harm. For these reasons, the Commission supports an approach that requires notice unless a company can establish that there is no reasonable likelihood of economic, physical, or other substantial harm.

VI. CONCLUSION

Thank you for the opportunity to provide the Commission's views. The FTC remains committed to promoting reasonable security for consumer data, and we are ready to work with this subcommittee as it develops and considers legislation on this critical issue.

Mr. BURGESS. The Chair thanks the gentlelady. Mr. Johnson, you are recognized for 5 minutes for the purpose of an opening statement.

STATEMENT OF CLETE D. JOHNSON

Mr. JOHNSON. Thank you very much. Dr. Burgess, Ranking Member Schakowsky, leaders of the full committee, distinguished members, thank you very much for having—for providing the opportunity to discuss the FCC's current programs and authorities regarding consumer protections for communications data, privacy, security, and breach notification. For decades Congress has recognized that information related to consumers' use of communications services is especially sensitive for reasons that go beyond potential economic harm, such as financial fraud or identity theft. If Americans can't communicate privately, if we are not secure in the privacy of information about our communications, then we can't fully exercise the freedoms and rights of open democratic society. As with medical and health care data, governed under HIPAA, and financial data, governed under Gramm-Leach-Bliley, and other statutes, Congress has long treated communications-related consumer information as a special category of consumer data that calls for expert oversight, tailored protections, and specific enforcement.

Given recent developments, the privacy and security of sensitive information held by communications networks is actually a much bigger issue now than ever before. For example, public concerns about the availability of telephone call records, the widespread use of fixed and mobile broadband communications, privacy implications of crucial life-saving improvements to next generation 911, and finally, recent cyberattacks, such as the one aimed at suppressing the release and viewing of a motion picture. As the expert agency that regulates communications networks, we continually seek to improve these protections for the good of communications consumers. I will now turn to the legal framework currently in place to protect these communications consumers, and also the responsibilities of communications providers to secure their networks in the first place. The draft bill would alter this legal framework significantly, and would leave gaps, as compared to existing consumer protections for communications consumers.

First, Section 222 of the Act establishes a duty for telecommunications carriers and interconnected VOIP providers to protect the confidentiality of consumers' proprietary information, including call records, location information, and other information related to the telephone service, such as the features of the customer's service, or even the customer's financial status. FCC rules under Section 222 require carriers to notify law enforcement and consumers of breaches, and carriers that fail to meet these requirements are subject to an enforcement action.

Second, Sections 631 and 338(i) apply to cable and satellite TV providers, and they protect consumers' viewing history. That is the TV shows they watch, and the movies that they order, as well as any other personally identifiable information available to the service provider. Here too the—these protections are enforced by FCC enforcement activity. And I would note that many of these protec-

tions, including those protections for several particular types of proprietary information, would no longer exist under the draft bill.

If enacted, Section 6(c) of the draft bill would declare sections of the Communications Act, as they pertain to data security and breach notification, to “have no force or effect”, except with regard to 911 calls. The Federal Trade Commission would be granted some, but not all, elements of the consumer protection authority that the FCC presently exercises. For example, if the draft bill were to become law, the FTC would not have the authority to develop rules to protect the security of consumers’ data, or to update requirements as new security threats emerge, and technology evolves.

Finally, while the draft bill attempts to maintain the protections of the Communications Act for purposes other than data security, the FCC’s experience implementing privacy and security requirements for communications consumer data shows that there is no simple distinction between these two interrelated concepts, privacy and security. Whether a company, number one, either by human or—human error or technical glitch, mistakenly fails to secure customer data, or, number two, if it deliberately divulges or uses information in ways that violated consumer privacy regarding that data, that—the transgression is at once a privacy violation and a security breach. In many cases it is the very same thing, and they—there—it is very difficult, practically or legally, to separate the two.

I thank you again for the opportunity to provide a summary of the FCC’s programs regarding data privacy and security, and, of course, look forward to answering any questions the subcommittee may have. We at the FCC, of course, stand ready, and willing, and able to provide any input or assistance the subcommittee may request as it completes this important work. Thank you very much.

[The prepared statement of Mr. Johnson follows:]

**Statement of Clete D. Johnson
Chief Counsel for Cybersecurity
Federal Communications Commission**

**Before the Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives**

**Hearing on
“Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015”
March 18, 2015**

Chairman Burgess, Ranking Member Schakowsky, distinguished Members, thank you for providing the opportunity to discuss the FCC’s current programs and authorities with respect to consumer protections concerning data privacy, security, and breach notification requirements for communications data.

Congress has recognized for decades that information related to consumers’ use of communications services is especially sensitive, for reasons that go beyond potential economic harm such as financial fraud or identity theft. If Americans cannot communicate privately, if we are not secure in the privacy of information *about* our communications, then we cannot fully exercise the freedoms and rights of an open and democratic society. As with medical and health care data governed under the Health Insurance Portability and Accountability Act and financial data governed under the Gramm-Leach-Bliley Act and other statutes, Congress has long treated communications-related consumer information as a special category of consumer data that calls for expert oversight, tailored protections and effective enforcement.

The privacy and security of sensitive personal information held by communications networks is a bigger issue than ever given recent developments, such as public concerns about the availability of telephone call records, the widespread use of fixed and mobile broadband communications, the privacy implications of important improvements to Next Generation 9-1-1, and recent cyber attacks, such as the one aimed at suppressing the release and viewing of a motion picture. As the expert agency that regulates communications networks, we continually seek to improve these protections for the good of consumers.

I would like to begin by discussing with specificity the legal framework currently in place to protect consumers and the responsibilities of communications providers to secure their networks in the first instance, and take remedial actions where data breaches occur. The draft bill would alter this legal framework and leave gaps as compared to existing consumer protections.

The Communications Act, through sections 222, 338(i), and 631 among others, establishes important consumer protections with respect to data security and breach notification. Specifically:

- Section 222 of the Act establishes a duty for telecommunications carriers and interconnected VoIP providers to protect the confidentiality of customers' proprietary information, including, but not limited to, call records, location information, and other information related to the service, such as the features of the customer's service, or even the customer's financial status. FCC rules promulgated under section 222 require carriers to notify law enforcement and consumers of breaches. Carriers that fail to meet the requirements of section 222 and its implementing rules are subject to an enforcement action brought by the FCC. Many of these consumer protections, including the protection of several particular types of proprietary information, would no longer exist if the draft bill were enacted.
- Sections 631 and 338(i), which apply to cable and satellite television providers, protect customers' viewing history – that is, the television shows that they watch and the movies that they order — as well as any other personally identifiable information available to the service provider. Consumers' privacy on these matters is also protected by FCC enforcement authority.

The FCC actively enforces the data privacy and security provisions of the Communications Act and related rules.¹ If enacted, Section 6(c) of the draft bill would declare sections of the Communications Act, as they pertain to data security and breach notification, to “have no force or effect” except with regard to 9-1-1 calls. The Federal Trade Commission would be granted some, but not all, elements of the consumer protection authority that the FCC presently exercises. For example, if the draft bill were to become law, the FTC would not have the authority to develop rules to protect the security of consumers' data or update requirements as new security threats emerge and technology evolves.

Finally, while the draft bill attempts to maintain the protections of the Communications Act for purposes other than data security, the FCC's experience implementing privacy and security requirements for consumer data reveals that there is no simple distinction between the two interrelated concepts. In short, whether a company (either by human error or technical glitch) mistakenly fails to secure customer data or deliberately divulges or uses information in ways that violate a customer's privacy rights regarding that data, the transgression is at once a privacy violation and a security breach.

I thank you again for the opportunity to provide a summary of the FCC's programs with respect to data privacy and security and I look forward to answering any questions you

¹ See, e.g., Sprint Corp., *Consent Decree*, 29 FCC Rcd 4759 (2014) (involving alleged violations of do-not-call rules); Verizon, *Consent Decree*, 29 FCC Rcd 10303 (2014) (involving alleged violations of CPNI rules).

may have. The FCC stands ready, willing, and able to provide this Subcommittee any assistance it may request in its important work to protect consumers in the 21st century.

Mr. BURGESS. Chair thanks both the witnesses for their forthright testimony. We will now go to the questioning portion of the hearing. I will recognize myself for 5 minutes for the purposes of questions.

Let me ask the same question to both of you. First, for the Federal Trade Commission, how many data security cases has the Federal Trade Commission brought to date? And, as a corollary, do you have an idea as to how many investigative hours have been spent on data security cases?

Ms. RICH. We have brought 55 data security cases, that is since the early 2000s, but we have actually brought hundreds of, combined, privacy and data security cases, held 35 workshops, completed 50 reports. We have spent—I actually haven't tabulated up man hours, but it is an enormous amount, because for every case we bring, there are actually quite a number of investigations that we look into, but we decide not to bring a Federal court action. So it is millions of hours.

Mr. BURGESS. OK, but the total cases was 55, was your response?

Ms. RICH. In the data security area, but many of the privacy cases have some data security element too, and there are hundreds of those.

Mr. BURGESS. Very well. Mr. Johnson, let me just ask the same question to you. How many data security cases has the Federal Communications Commission brought, and then, likewise, the investigative hours that your commission has spent on the data security cases?

Mr. JOHNSON. Thank you, Mr. Chairman. In the 18 years that Section 222 has been in place, and this is the section that pertains primarily to telephone call records, there have been—I don't have the precise number, but I think it is in the realm of scores and scores of cases that pertain to what is called customer proprietary network information. This is call records, location information, time and duration of call, and a whole host of other what is called CPNI protections. I don't have the precise number, and I can certainly get you the precise number, nor the total accumulated hours, but it is scores and scores.

Mr. BURGESS. To the extent—I think it would be helpful to the subcommittee if you could make the actual numbers available, and certainly—

Mr. JOHNSON. Of course.

Mr. BURGESS [continuing]. I would allow you to do that for the record. Let me just ask you a question. You brought up the Consumer Proprietary Network Information. How many years after the 1996 Act did it take to fully implement the rules for CPNI at the Federal Communications Commission?

Mr. JOHNSON. Well, I think that that—I don't know which exact rule you are referring to, Mr. Chairman, but I think the broad answer is that it has been underway for 18 years, and there have been multiple improvements and shifts, including for Congressional expectation, technological development, for instance, voice over IP, location information that pertains to 911. And in 2013 there was a declaratory ruling that the Commission declared that CPNI pertains to information that is collected on mobile devices.

So I guess the accurate answer is that it remains a work in progress, and that is part of the value of having that rulemaking authority, is in order to adapt to Congressional expectations, changes of technology.

Mr. BURGESS. Maybe for the purposes of clarification for the subcommittee, as we work through some of these issues, could the Commission provide us a timeline, from 1996 to present, where the rulemaking was involved, where it evolved? Obviously the threat changed over that time as well. But I am—I guess, you know, that is part of my concern, is that it—I get the impression that it took some time from '96 to the point where the rulemaking had evolved to a point where there were actually consumer protections that were available. But I don't know that, and you are——

Mr. JOHNSON. Absolutely. I will take that—I think that is a very important homework assignment for me, and I—run through very briefly—the section was established in 1996.

Mr. BURGESS. Right.

Mr. JOHNSON. In 1999 location information was added. In 2007 there was a major problem with what is called pre-texters. And in my old world in—working on intelligence policy, this is essentially a human intelligence collector, where pre-texters would call the telephone company, ask——

Mr. BURGESS. Right. We had a hearing on it here in this committee several years ago as well.

Mr. JOHNSON. And so that was something, again, that was at once a privacy and security issue, and in 2007 the Commission issued rules specific to solving that problem. And, again, there have been some other adjustments and improvements in recent years. But we will get you the full story. It is actually—it is—it is an important story about the development of Section 222.

Mr. BURGESS. The Chair appreciates the gentleman's willingness to provide the information. The Chair recognizes Ms. Schakowsky. Five minutes for questions, please.

Ms. SCHAKOWSKY. I just want to clarify that my concerns between the agencies is really with regard to the impact on consumers. I don't want anything I say to seem to reflect a preference for one agency over another, but rather for the protection of the consumers.

So my—if this draft were enacted, regulatory and enforcement authority over data security and breach notification that is currently granted to the FCC would—under certain sections of the Communications Act and its regulations would have no force or effect. It is my understanding that the data security and breach notification protections under the Communications Act are broader than the protections afforded under this draft. The Communications Act provides security protections for information regarding telecommunications subscribers' use of service, but this draft does not provide security protections for all of that information. Instead, it covers only "the location of, number from which, and to which a call is placed, and the time and duration of such call".

So, Mr. Johnson, what other information is currently protected under Title II of the Communications Act that would not be covered under this draft?

Mr. JOHNSON. Ma'am, you are correct it—that there are specific pieces of information, both under Section 222 and also the cable/satellite provisions, that are not protected under this draft. With regard to Section 222, information such as how many calls a person has made, you know, sort of the peak calling periods for that person, does this person make phone calls in the morning, at night, lunchtime, specific features of the service, like call waiting, caller ID, and then other things that may be pertinent to call service, like the financial status of the customer. Is the customer—does the customer qualify for Medicaid, or SNAP, or other low income support? Those would explicitly not be protected by the definition in the draft bill.

On the cable and satellite side, it is—essentially all of it would not be protected. What television shows you watch on cable and satellite, what pay-per-view you order, what you order from the Home Shopping Network, none of this would be protected under the draft bill, and it is—

Ms. SCHAKOWSKY. So—

Mr. JOHNSON [continuing]. Presently protected.

Ms. SCHAKOWSKY. So viewing preferences, or viewing history, none of that would be covered?

Mr. JOHNSON. It is presently covered. It would not be covered under the draft bill.

Ms. SCHAKOWSKY. No, that is what I am talking about. This bill also voids breach notification obligations required under the Communications Act, Mr. Johnson, and its regulations, but as I read it, the bill would not require breach notification for a breach of call information. Under the Communications Act, and associated regulations, a breach of customer information, such as call data and viewing habits, requires notice to law enforcement and affected customers. Is that right?

Mr. JOHNSON. That is correct.

Ms. SCHAKOWSKY. But as we established, much of the customer information currently required to be secured under the Communications Act does not have to be secured under this bill. And if there is no requirement to protect the information, then there is no requirement to provide notice in the event of a breach, correct?

Mr. JOHNSON. That is correct.

Ms. SCHAKOWSKY. And even for the limited call information that must be secured under this bill, a breached company would not be required to provide notice because call information is not financial in nature, do you agree?

Mr. JOHNSON. That is my interpretation, yes, ma'am.

Ms. SCHAKOWSKY. So I wondered, Ms. Rich, if you wanted to comment on that. This is a concern that I have for consumers, that I think if we allowed the FCC to continue in its regulations, that we could then make sure we cover everything.

Ms. RICH. We—for consumers—we are also looking at this bill in terms of its effect on consumers, and that is why, in our testimony, we have proposed that the bill apply to more information, geo, health. Communications would also be something that should be added to the bill. We also believe the breach notification trigger should be a bit broader to encompass different harms. So that, we agree, would be an improvement to the bill.

But I—as to jurisdiction, I should say that our position is that we should have jurisdiction in this bill. The FTC should have jurisdiction over carriers in this bill because we have brought so many cases in this area. We bring so much enforcement expertise to the table. We really have been working on this issue since, really, the mid '90s. We also believe we should be able to hold different companies that are collecting some of the very same type of information to the same standards on—in our enforcement. You know, Netflix, Google, and Verizon really have a lot of the same information.

And, further, the—we haven't taken a position on reclassification, but one byproduct of reclassification is it does remove our FTC jurisdiction from over providers of broadband service, so we would actually be—we are actually able to do less post-reclassification to help consumers than we were able to do before. That being said, we believe—a majority at the Commission believes we should share jurisdiction with the FCC, and not displace the FCC.

Ms. SCHAKOWSKY. Thank you. I yield back.

Ms. RICH. We work very well together.

Ms. SCHAKOWSKY. Thank you.

Mr. BURGESS. Gentlelady's time has expired. The Chair recognizes the gentleman from Michigan, the chairman of the full committee, Mr. Upton. Did he—Ms. Blackburn, then, you are recognized to have 5 minutes for questions, please.

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I want to thank our witnesses for being here.

Mr. Johnson, to you first. Please get your facts and figures all in order, as Chairman Burgess asked, and get that back to us. It is helpful—

Mr. JOHNSON. Yes.

Mrs. BLACKBURN [continuing]. To us, and we were hopeful to have that information today to be able to define the number of data security cases that you all have brought forward, not just terming it “scores and scores.” So let us tighten that up for the record.

Ms. Rich, to you, you talked about the 55 cases that you all have brought forward, so I want you to walk me through what is the criteria that you utilize when you decide to bring a case forward? What is—what goes into that decision matrix?

Ms. RICH. The core concept in our data security program, whether—and we have several different laws we enforce, is reasonableness, and not whether there has been a breach. And we have emphasized a process-based approach that is tech neutral. So for years our education and our cases have been emphasizing that the key to data security is to follow certain key, you know, basic common elements, put somebody in charge, make somebody responsible for the program, do a risk assessment to determine what are the risks in your business, not some checklist that another business with a totally different business model is using, develop a program to address the risks you have just found, and focus in particular on things like the key area—

Mrs. BLACKBURN. Let me interrupt you there.

Ms. RICH. Yes.

Mrs. BLACKBURN. Would you consider, then, that you all have an informal set of best practices that you refer back to? Would that be a fair statement?

Ms. RICH. Yes. It is not really informal, because it has been widely publicized in the education materials we put out in our complaints and orders, which all re-iterate these same elements.

Mrs. BLACKBURN. OK. All right. Let me ask you this, then. Do you think the draft legislation would limit the FTC's Section 5 authority?

Ms. RICH. Well, there is a savings clause, and we are happy about that, but, you know, as we understand it, this is a discussion draft, and so right now we have some concerns that it might weaken the protections that are currently in place. But with some of the suggestions we have made for strengthening the bill, we believe it could be quite strong.

Mrs. BLACKBURN. OK. So you would rather—OK, let me ask you about this, then: What about consent orders? You all have to go ahead and get that consent order to obtain civil penalties for unfair or deceptive practices, so do you believe consent orders are a strong incentive for industry for instituting data security civil penalties?

Ms. RICH. You are making an excellent point, which is that the bill's inclusion of civil penalties is critical, and we are very supportive of that. Right now, as you note, in order for us to obtain civil penalties, which believe are an important incentive and deterrent from bad behavior, we have to obtain an administrative order first, and then, if there is a violation, obtain civil penalties. So yes, you are absolutely right, that civil penalties are a key ingredient to the success of legislation.

Mrs. BLACKBURN. OK. With that, I am going to yield back my time, Mr. Chairman, so we can move on with the rest of the questions.

Mr. BURGESS. Appreciate—the gentlelady yields back. Chair recognize the gentleman from Massachusetts, Mr. Kennedy, 5 minutes for questions, please.

Mr. KENNEDY. Thank you, Mr. Chairman. And, again, thank you to the witnesses for testifying. I appreciate the information that you have already offered us today, and as we go through this process.

The FCC has enacted strong regulations to implement their authorities under the Communications Act, and I know you have touched on that a little bit already. These regulations require telecommunications providers to implement a number of specific privacy and security measures to protect consumer proprietary information. I wanted to walk through, with both of you, a little bit about some of those requirements so we can flesh this out a little bit.

So, Mr. Johnson, these regulations require that telecommunications carriers take steps not only to secure customer information, but also discover attempts to gain unauthorized access to that information, isn't that right?

Mr. JOHNSON. That is correct.

Mr. KENNEDY. So carriers also, then, must authenticate a customer before providing customer information over the phone, online, or in a store as well?

Mr. JOHNSON. That is correct.

Mr. KENNEDY. Carriers are required to train their employees in the use of that customer information, is that right?

Mr. JOHNSON. That is correct.

Mr. KENNEDY. OK. Are there some other things that are required under the FCC's regulations that you would like to highlight as well?

Mr. JOHNSON. In addition to those that you laid out, Congressman, carriers are also required to discipline abuses and to certify compliance with these rules. And, if I may, I would add to that the distinction between enforcement and rulemaking clarity. Of course enforcement is a crucial part of compliance, and the FCC has an Enforcement Bureau that is very active in this space, as is the FTC in the—we partner together on—in many areas, and expect to in the future as well.

The distinction between the present protections in 222 and an enforcement only approach is that the FCC, or in this case, the FTC, if this bill were to be enacted, the FCC presently has the ability to get out and engage the public, the providers, to work together through advisory committees, through rulemaking processes, through a whole host of measures, to make clear what the challenges are and what the solutions are before there is a problem. So instead of post hoc enforcement only, there is a solving the problem before it happens, or once it has been spotted, in the case of pretexting, Mr. Chairman, that you can go after this problem, and seek to solve it, instead of just post hoc—

Mr. KENNEDY. So proactive versus reactive, right?

Mr. JOHNSON. That is right.

Mr. KENNEDY. So would those requirements be preempted under the current legislation?

Mr. JOHNSON. They would be eliminated.

Mr. KENNEDY. So, Ms. Rich—thank you, Mr. Johnson. Ms. Rich, if, for example, a telecommunications provider disclosed the number of calls that I made from a specific phone number to a third party, would the FTC be able to bring an enforcement action under this bill?

Ms. RICH. We believe that should be added to the bill.

Mr. KENNEDY. OK. And would the FTC be able to require that telecommunications providers not disclose that information unless they obtain customer consent, or should that be added as well?

Ms. RICH. Well, that would be a privacy provision, so I am not sure it would be addressed by this bill. But—and I don't think that would be preempted by this bill, the privacy provisions of the CPNI rules. But, in any event, we do think communications should be added to the bill as an element—a data—a piece of data that should be covered.

Mr. KENNEDY. OK. I appreciate the feedback. Thank you very much, and I yield back.

Mr. BURGESS. Gentleman yields back. The Chair now will recognize the vice chair of the subcommittee, Mr. Lance. 5 minutes for questions, please.

Mr. LANCE. Thank you, Mr. Chairman. Good morning to you both.

To Ms. Rich, the FTC has been a strong advocate for protection of Social Security Numbers, and has often indicated that Social Security Numbers are closely tied to identity theft. I don't think there is any doubt about that. How many State data security and breach notification bills include Social Security Numbers alone as personal information?

Ms. RICH. We have that information, but I don't have it at my fingertips, but we would be happy to provide it to the committee.

Mr. LANCE. Thank you very much. Mr. Johnson, did you have an opinion on that?

Mr. JOHNSON. I don't know the answer to that—

Mr. LANCE. Certainly. Thank you. To Ms. Rich, do you support the inclusion of standalone Social Security Numbers as personal information in the draft legislation?

Ms. RICH. Yes. We were very happy to see that in the bill.

Mr. LANCE. Thank you. And are these data elements not listed in the draft legislation that the FTC has seen tied to identity theft and payment fraud? Are there any data elements not listed in the draft legislation that you would like to see in it?

Ms. RICH. Yes. In addition to Social Security Number, driver's license and passport number, and other Government-issued numbers can also be used to perpetrate identity theft, so we would like to see that information protected standalone, and now it needs to be coupled with other information.

We have also believed that health insurance numbers can lead to medical identity theft, where people place charges in hospitals billed to other people, and it can really accumulate, and they can do that with simply health insurance numbers. And I believe those are the main elements, besides health and geolocation, which we are not talking about identity theft, we are talking about other information that should be protected. But those are the main additional elements.

Mr. LANCE. So, to reiterate, other than Social Security, driver's license, and then health identification numbers?

Ms. RICH. Yes.

Mr. LANCE. Thank you. Mr. Chairman, I yield back the balance of my time.

Mr. BURGESS. Chair thanks the gentleman, the gentleman yields back. The Chair recognizes the gentleman from Vermont, Mr. Welch. Five minutes for questions, please.

Mr. WELCH. Thank you very much. And I thank the witnesses for your very helpful testimony. Just by way of introduction, I think we have got some areas of real agreement here. Number one, bipartisan agreement that this is a brutal problem. Number two, it is the Wild West. There is no clarity about who is in charge, or what the enforcement is. Number three, there is a desire to get things done that are going to add protection, rather than take it away.

There is some disagreement on policy matters. Like, for instance, you, Ms. Rich, indicated you want, as you call it, a stronger trigger notice, and where that balance is—you used that word, balance, that is a debatable proposition. You know, I happen to think that the notice provisions under Gramm-Leach-Bliley—I don't know if you have refinanced your mortgage at all, but you get so much in-

formation it is useless, so I want to balance where consumers are protected and notified but not terrified, and that is a discussion in a debate.

But there are other areas where—for instance, with Ms. Schakowsky, she raised what I thought were some really valid concerns, and this is with respect to the transition of authority. Because my view of the language is that the CPNI that would go to the FTC, you would have that enforcement authority. And the bottom line for me is the concern, which I think is what Ms. Schakowsky was expressing, do we protect the consumers, as opposed to who is in charge.

And I actually do share that, but the privacy provisions that you were talking about, Mr. Johnson, my understanding, and I think, Ms. Rich, you testified to this, the privacy provisions that FCC has would be retained, and not preempted, correct? That is your view, Ms. Rich?

Ms. RICH. I would defer to my colleague on that.

Mr. WELCH. No, I want to ask you, because if we have, essentially, a situation where we think we are in agreement, but we have language that we are uncertain meets the agreement that we think we have, then that is a different—the nature of that is a different challenge. It is like trying to get the language right. And I appreciate Ms. Blackburn and Mr. Burgess for focusing on, you know, trying to define what the problem is, rather than create additional problems. But my understanding of your testimony was that you believe that privacy was not preempted, correct?

Ms. RICH. If I have the current version of the legislation, I thought I saw in there that the privacy provisions of the CPNI rules, and other portions of the Communications Act, were retained.

Mr. WELCH. Right. And, Mr. Johnson, is that your view as well?

Mr. JOHNSON. Yes, sir. I do think that that is—the language attempts to divide privacy from security.

Mr. WELCH. All right. So let us say we got the language right to your satisfaction, and the FTC took over authority for CPNI, and you retained—the FCC retained the current jurisdiction it has for privacy. From an agency standpoint, that might not be your preference, but from a consumer standpoint, you would still be holding folks harmless with a new enforcer on some of the elements, is that right?

Mr. JOHNSON. Sir, I would actually say that it is not possible to divide privacy from security, because in most cases the security of information is the privacy of the information, and vice versa. So, for instance, if you have an insider threat, if there is a bad actor in your company, or a mistaken actor in your company, and that person has authorized access to the information, but then mishandles it, or commits some sort of—

Mr. WELCH. OK, I am—I appreciate that, and I am going to ask you to help us here, because the spirit that our chairman has provided here I think is really good. The big problem for everyday people in Vermont is their financial information. A lot of these other things that you have mentioned, they are important, and we have got a lot of work in this Congress to deal with privacy questions—

Mr. JOHNSON. Um-hum.

Mr. WELCH [continuing]. But 90 percent of the problem for 100 percent of the people is loss of their identity and their financial information. And, you know, the bad guys out there, that is what they want.

Mr. JOHNSON. Um-hum.

Mr. WELCH. If they want my Social Security Number, it is not for any reason other than to get to my bank account.

Mr. JOHNSON. Right.

Mr. WELCH. So I think the focus here of a narrow approach that Mr. Burgess has adopted, I think, makes some sense. Now, if there—we don't want to lose rights that people have, but we may need the help of the FTC and the FCC to write that language so that we accomplish this goal that we are accepting is narrow, but without compromising other rights.

Mr. JOHNSON. I——

Mr. WELCH. So——

Mr. JOHNSON. And I—if I may, sir, I, of course, commend you, and all of you, for trying to tackle this issue. When I was a Senate staffer on the other side, I tried it as well, and we didn't quite get there. The two things with regard to consumer protections that I would like to mention are, number one, with regard to communications consumer protections, it is a different type of information.

And I think you will hear in this next panel some very expert, knowledgeable witnesses say that data is data, a server is a server, and I would just respectfully disagree that, with regard to call data, with regard to data that flows over networks, cable/satellite, it is specific to the network engineering, and how these networks actually——

Mr. WELCH. All right. My time is running out, but here is the one request I am going to make of you. You have identified a problem. We need you to identify a solution, because this is not a policy difference that you are describing now. This is a practical challenge that you are describing. Let us get your help in solving that.

Mr. JOHNSON. Absolutely.

Mr. WELCH. I yield back.

Mr. BURGESS. Chair thanks the gentleman. Gentleman's time has expired. The Chair recognizes the gentleman from Texas, Mr. Olson. Five minutes for questions, please.

Mr. OLSON. I thank the Chair. Welcome, Mrs. Rich, and Mr. Johnson. Sadly, data breaches have become common news. Just this morning we learned about Primera Health Care. 12 million of their customers lost their data, had it exposed to hackers. They were attacked in May, discovered the attack in January, and found out recently what had happened. We can do better, but we need to take a balance approach to data breach notifications. We have to protect consumers, but we can't be a burden to companies and hinder the legal uses of data.

This draft doesn't fix all the problems, but it is a small but important step in the right direction. I have a few questions for you this morning. The first ones are for you, Ms. Rich. How many people work in your division in the FTC?

Ms. RICH. We have a privacy division of about 45 people, but we have a number of regional offices, and a number of other offices

that work on various privacy issues, like Do Not Call, or privacy issues related to financial information, so we have quite a number of people working on privacy. We, of course, could always use more, but—yes.

Mr. OLSON. How many folks on data security? All 45, or more than 45? And how many people focus on data security within the FTC, or your division?

Ms. RICH. I don't have at my fingertips exactly, but almost everyone in the division works on both privacy and data security. And then, as I said, there are people in other parts of the agency who also work on these issues. So—I can get you more information, if you would—

Mr. OLSON. Thank you.

Ms. RICH [continuing]. Like, but—yes.

Mr. OLSON. Do they determine what a reasonable data security practice is? Do they do that, as a matter of policy?

Ms. RICH. We have standards that we have put out, both in our original Gramm-Leach-Bliley safeguards rule, in all of our complaints and orders. As I said, we lay out a process that is reasonable security. We consider, you know, various factors, like the sensitivity and volume of data, et cetera, and the staff attorneys who work on this follow the standards that we follow throughout the agency, and that we have announced to the public in particular cases.

Mr. OLSON. Do they make sure companies use good practices? If so, how do they do that, ma'am?

Ms. RICH. We—in investigations, we evaluate whether reasonable security was followed, and whether these types of processes I talked about was—were followed.

Mr. OLSON. And I am sure you have to have people with very special skills. How hard is it to find those people? Is that a problem for you, ma'am, need more people with the skills to go after these hackers?

Ms. RICH. We have very well trained attorneys and investigators. We also have a lab unit that helps with—if there is any forensics involved. And we have experts and technologists, both on staff, and that we consult with.

Mr. OLSON. Thank you, Ms. Rich. Mr. Johnson, for you, my friend, how many folks in your department work on data security? Not cybersecurity, but data security, within the FCC?

Mr. JOHNSON. Congressman, I can get you a specific answer. It is not divided quite as neatly for us as it is at the FTC, in the Consumer—

Mr. OLSON. Ballpark, 10, 20, 30?

Mr. JOHNSON. I would say dozens of people work on various aspects of this in the Public Safety Bureau, that is the bureau that I am in, in the Enforcement Bureau, also the Wireless Bureau, the Wire Line Bureau, the Media Bureau. It is an issue that covers—in the Consumer Protection Bureau, essentially every bureau of the FCC has a role in this in some form or fashion.

Mr. OLSON. And how about finding really qualified people? Hard time finding the people and skills you need at the FCC to do your job with these data breaches?

Mr. JOHNSON. I would say that the FCC is—has the most qualified network engineers and communications lawyers, and, importantly, communications economists that I have run across. It is an expert agency in the communications field.

Mr. OLSON. So it sounds like you balanced enforcement with the market, communications, economics, and so you are actually a partner in this endeavor, so thank you for that. I am out of my time. Yield back.

Mr. BURGESS. The Chair thanks the gentleman. The Chair now recognizes the gentleman from Illinois, former chairman of the subcommittee, Mr. Rush. Five minutes for questions, please.

Mr. RUSH. Thank you, Mr. Chairman. I really am enjoying the input, and the conversation both ways, in regards to this particular matter. I view the issue before us as an issue that is really—that we have to maintain the understanding that data security and privacy are really like two sides of the same coin, and we can't bifurcate these two issues.

I think we have to proceed with, really, the understanding that, in order to be forced to really serve the American people, and begin to deal with this issues—these issues that they are confronted with, both in terms of privacy and also data security, that we can't waste our time in trying to separate these two issues. And I don't think the outcome would be an outcome that we want to achieve, and that would really help us out in the problem that all of us are vitally concerned about.

I want to ask Ms. Rich, recently the FC announced that broadband providers would be regulated as common carriers. Under these particular rules, if a broadband provider were to be the subject of a data breach, which agency would have primary responsibility for ensuring that any Federal standard is enforced? And, Mr. Johnson and Ms. Rich, I want you to answer those question—this question, beginning with you, Ms. Rich.

Ms. RICH. Prior—we have not taken a position on reclassification generally, but, as I mentioned, a byproduct of it is we—it limits our ability to protect consumers when the companies that perpetrate the violations are broadband providers. So if a broadband provider had a breach, and it was—pertained to their provision of broadband service, and not some ancillary service, we would no longer be able to protect service in that area. We would like, of course, to have somebody, maybe somebody here, restore that jurisdiction to us. We don't, however, object to the reclassification.

Mr. RUSH. Mr. Johnson, what are your—

Mr. JOHNSON. Congressman—

Mr. RUSH [continuing]. Comments?

Mr. JOHNSON. We are—my focus in work, and also at this hearing, is the—is—are the provisions that pertain to data security of communications data. I am certainly aware of the effect that Title II reclassification has, particularly on Sections 201, 202, and 222. And, if it is OK with you, I will leave it at that, because I have never practiced law with regard to the Federal Trade Commission Act, and I will defer to the Federal Trade Commission, and—

Mr. RUSH. OK. Well, thank you so much. Ms. Rich, can you clarify one piece of your testimony, if you will? You are advocating to lift the common carrier exemption, but not to take away regulatory

or enforcement authority from the FCC, am I correct? That is—how would that be done? What do you suggest?

Ms. RICH. Well, we share jurisdiction with a lot of different agencies in a lot of different areas, and, you know, we have—for example, with the CFPB, we have an MOU with them. We have, for years, shared jurisdiction with the FCC as to do not call. We did share jurisdiction over broadband providers, proprietor re-classification, and we can successfully coordinate, and make sure there is no duplication.

So what we are saying is we think, as the agency that is most experienced in the data security area has can be very effective in protecting consumers that we should be—we should have jurisdiction over carriers, but that we—that the FCC—the majority of our commission believes that that doesn't mean the FCC shouldn't—should be displaced in its jurisdiction.

Mr. RUSH. OK. Is there—in terms of the—your practice that you have regarding these memorandum of understandings, does that create a burdensome issue for the consumer? Is there—does that complicate their lives, or—

Ms. RICH. No, not for the consumer at all. In fact, the consumer potentially has two cops on the beat. But what the MOUs and the coordination is usually for is to make sure that there is no duplication and burdens created for businesses. For example, the two agencies, without communicating with each other, both investigating the same company at the same time.

Mr. RUSH. Mr. Johnson, you want to comment on—

Mr. JOHNSON. I think she stated it very well, sir.

Mr. RUSH. Mr. Chairman, thank you, and I yield back.

Mr. BURGESS. Chair thanks the gentleman, the gentleman yields back. The Chair recognizes the gentleman from Kansas, Mr. Pompeo. Five minutes for questions, please.

Mr. POMPEO. Thank you, Mr. Chairman, and thank you both for being here today. I suppose I am not surprised, but I am troubled by how little conversation there has been this morning about cost to consumers. When you talk about protecting consumers, there is very little discussion about what this will mean, right? If a business is paying money, it gets passed along, and there is just remarkably little discussion about what it really means to someone who can least afforded whatever services that we are dealing with. I think that is very important.

I would hope that the two of you would appreciate that too, but instead what I get is two Government agencies, each of which wants increased authority, increased power, more control, the capacity to define rights, sort of the historic governmental actions. I would hope, when you think about the consumers that you are tasked to oversee that you would at least consider their economic well-being as well.

Ms. Rich, in that vein, you have asked for a—you said that the definition contained—really, the notice provision, you weren't happy with it. You suggested alternative language. You said you would support an approach that “requires notice, unless a company can establish there is no reasonable likelihood of economic, physical, or other substantial harm”. So you have flipped the burden of proof now to the consumer, right? Right, to the business which they

have contracted with to demonstrate that there is no harm. What do you think the cost of a change like that would be?

Ms. RICH. I think the burden is already flipped in the draft. All we are proposing is that the—instead of it being limited to financial harm, that it be—include economic, physical, or other substantial harm.

Mr. POMPEO. Fair enough. I want to go on to Mr. Johnson. Mr. Johnson, you—I think in response to a question you said that there were—you didn't know the exact date, or you were going to bring us that, but you said there were scores of cases? Is that right?

Mr. JOHNSON. Yes, sir, of—

Mr. POMPEO. That you brought? And you identified two in your written testimony, if I got it right. Is—

Mr. JOHNSON. I think the—if I remember correctly, the two that are in the footnote in the written testimony—

Mr. POMPEO. Right.

Mr. JOHNSON [continuing]. Were just two examples from last year that were concluded. I—we are—I would draw a distinction between cases that are investigated, cases that are pursued, cases that are settled, and not necessarily cases that all end in a—

Mr. POMPEO. Are these the only that have—that are of record? You said there are “scores and scores.” There are two identified. Are there others that you could have put in this—

Mr. JOHNSON. Absolutely. Yes, sir, and I committed earlier—

Mr. POMPEO. And would any of those have actually been data breaches? Because neither of these, as described in your testimony, are actually what we are dealing with here today.

Mr. JOHNSON. Well, I think the—

Mr. POMPEO. One is a Do Not Call case, according to your testimony, and one was a violation of—

Mr. JOHNSON. Yes, sir, your question underscores the distinction that we think is important with regard to communications data. It is not just breach of Social Security Numbers or credit card numbers. It is information about what people do on the telephone, what do they do with cable and satellite TV, and it is a much broader set of data that is specific to the networks that hold, and manage, and deliver that data.

So it is harder for us to hone in on, this was a data breach of Social Security Numbers, than it is to talk about how we prospectively and proactively protect the consumer in a way that is actually, I think, to your original point, is cost effective, because it allows us to engage ahead of time with the providers. And I can give a number of examples about how we do that in a way that aligns it with business interests to protect the consumer, while also letting the companies sort of—

Mr. POMPEO. Yes.

Mr. JOHNSON [continuing]. Lead the solutions, yes.

Mr. POMPEO. I am not sure I agree with you. I went back and read the Notice of Apparent Liability that you have issued, and the language you used implies that if you have a breach, then your security is, per se, unreasonable, and your privacy policy is deceptive. Is that the FCC's position?

Mr. JOHNSON. I don't know the exact line that you are going at there, but do you know which action you are referring to, sir?

Mr. POMPEO. I do, but I want to go more generically. I want to kick it out from the particular case. Is it the case that it is the FCC's view that it is, per se, unreasonable, and your privacy policy is deceptive, if there was a breach?

Mr. JOHNSON. No, sir, I don't think that is the case. In fact, in our rules, on the 222 side, it requires reasonable measures to discover and protect against unauthorized access.

Mr. POMPEO. Great. Thank you. Mr. Chairman, my time is up. I yield back.

Mr. JOHNSON. If I might, sir, the one additional note is that on the cable/satellite side, and this is another distinction with the bill, the standard is not just reasonable. It is as necessary to protect, so it is a much higher standard in the cable/satellite viewing preferences case.

Mr. POMPEO. Thank you.

Mr. JOHNSON. But I wouldn't say it is a per se violation.

Mr. BURGESS. Chair thanks the gentleman. Gentleman's time has expired. The Chair recognizes Mr. Cárdenas. Five minutes for questions, please.

Mr. CÁRDENAS. Thank you very much, Mr. Chairman. I want to thank the witnesses for all of your service. It is an issue that is becoming more and more important. But one thing that I would like to underscore is that I look at this as similar to what we all, as Americans, thankfully, take for granted, that in any community we have Government police. And let me tell you, when communities hire private policing, or what have you, talk about things getting out of control, and talk about lowering the standard of the kind of security that community has.

There is certainly a drastic difference between hiring a security guard versus calling 911 and having the true police force show up. So I want to thank both of you, and both of your departments, for what you do for us to keep us safe. And certainly to keep the cost effectiveness of your purpose I believe is about American consumers, and making sure that we fortify you with the resources you need so you can have the intelligent individuals, and the hard-working individuals to go ahead and make sure that breaches don't happen as often as possible, we can be preventative.

Because let me tell you, what we pay in taxes is nothing compared to the person who gets their information breached. They lose their house, their entire credit report goes to the wastebasket, and they lose everything. And then in many, many cases it is years and years and years before that individual, or that family, can actually get back to being right, and their entire reputation is, again, goes to the wastebasket. As far as on paper, people think of them, because their bank account was cleaned out, they couldn't pay their mortgage, they lose their home, they can't run their business, or what have you, because they no credit, they can't get access to capital, et cetera. So let me tell you, when you—when we allow you to do your job well, I think that less and less of that does happen to our American public.

So, with that, I only have time for perhaps one question. I want to refer back to the—FTC recently released a staff report on Internet of things. The Internet of things refers to the ability of devices to connect to the Internet, and send and receive data. As the report

acknowledges, many of these devices are vulnerable to being hacked. About 60 percent of web enabled devices have weak security, and that is what has been reported.

In September of 2013, the FTC took its first action against an Internet of things company when it brought a complaint against TRENDnet, a company that manufactures web-enabled cameras, for misrepresenting the security of its cameras. In that case, it was not personal information in electronic form that was accessed, but rather live feeds from the cameras, including the monitoring of babies.

So, Ms. Rich, do you agree that reasonable security measures include implementing procedures and practices that limit the ability of hackers to remotely access control Internet connected devices?

Ms. RICH. Yes. You have touched on two things that are very important to us about this bill. First, device security. That is—it is because of our work on the Internet of things that we realized that it is very important to security devices so they can't—even regardless of the personal information involved, they can't be taken over and used in ways—for example, medical devices that—or automobiles, which I discussed in my—at the beginning to hurt consumers.

And also, TRENDnet—our case against TRENDnet was an example where it wasn't financial data that was exposed, it was pictures of very private things happening in homes, and that kind of sensitive information does need to be protected.

Mr. CÁRDENAS. OK. Thank you. Ms. Rich, what type of access control measures would limit the ability of hackers to remotely accessing controlled devices, and how could companies implement those measures to make consumers safer?

Ms. RICH. We believe the legislation should actually just include a reference to protecting device security in order to make sure the—that is—that devices are protected from that kind of interception.

Mr. CÁRDENAS. And also, generally, are the people who have been attempting to hack, and it is my understanding that it is in the millions and millions of attempts per year on American companies, and on our Government, et cetera, are those hackers limited in their budgets? Do they seem to have a limited budget per year, and they stop doing what they do, and they wait until next year's budget?

Ms. RICH. There are very sophisticated hackers out there who are very motivated, and many of them aren't even in this country. And many of them do these—they are so good at what they do, they don't actually require a huge budget.

Mr. CÁRDENAS. OK. I don't know if we could ever even the playing field, but I would love to see that we fortify you with the resources you need to protect us. Thank you very much, Mr. Chairman.

Ms. RICH. Can I just add something? I want to make sure—I feel like I have been too modest in the way I described our 55 cases, because those were completed cases that ended in an order. And if we did include investigations, and all of the—and closing letters, and all of the activity we engage in that doesn't lead to a signed order, there are hundreds of data security cases.

Mr. BURGESS. The Chair thanks the gentlelady for the clarification. The Chair now recognizes Ms. Brooke from Indiana. Five minutes for questions, please.

Mrs. BROOKS. And I want to thank all of the witnesses for valuable time educating the public, educating all of us on the proposed changes to further safeguard sensitive consumer information by providing the timely to these individuals. Also want to commend the chairman on all the work that has been done. As a new member to Energy and Commerce, I know there has been a lot of work done over the years, and, obviously, the growing nature of cyberinfrastructure in all of our lives, it makes this so very important.

I have to tell you, we did—before the hearing today, in 2014 alone, the Indiana Attorney General's Office received more than 370 data breach notifications, and more than 1,300 identity theft complaints in Indiana. Actually—that was, actually, I thought, kind of low, considering many of us have just received notification from our insurance company about the breach in Indiana of potentially up to 80 million customers.

But I want to ask, from your perspective, Ms. Rich, at the FTC, how does a national security standard in the draft bill—wouldn't a national security standard help consumers, in theory? And—because I am not hearing that you are interested in a national security standard, but that, in fact, we should continue to allow 47 to 50 different State standards to be in place. Talk to me about a national security standard, and what, you know, what your thoughts are on that. Because I am not hearing that you are in favor of that.

Ms. RICH. We absolutely agree that a national security standard would be helpful. It would make very clear what the expectations are. It would fill the gaps, not—only 12 States have data security laws, even though 47 have data breach laws, if I am up to speed on all the laws that have passed. But we—

Mrs. BROOKS. Could you—

Ms. RICH. We absolutely—

Mrs. BROOKS [continuing]. Explain to us the distinction between data security laws versus data breach laws?

Ms. RICH. I just want to qualify what I was saying, and then I definitely—

Mrs. BROOKS. OK.

Ms. RICH [continuing]. Will. But we are concerned about a national standard if it would water down protections that are currently in place today, which is why we are suggesting some modification to this discussion draft to strengthen it, so that it wouldn't weaken the protections in place today. Because if it preempts the State laws, and the main thing there is health. To preempt State laws that provide data security for health information, and that is already provided now, then there won't—there would be fewer protections for health information. So that is our concern. But yes, in theory, we absolutely do support a national standard.

In terms of the difference between data security and data breach, data security is protecting the data so there isn't a breach. And, in fact, the FTC's focus has been chiefly on that, not as much breach notification, in part, because we don't have breach notification authority, except in a narrow area. So data security is very, very im-

portant, and that is why, right at the outset, I thanked the subcommittee for including data security, and not just data breach notification, which is, you know, after the breach happens you tell consumers, but the horse is already out of the barn.

Mrs. BROOKS. Can you explain—in your prepared testimony you talked about it is critical that companies implement reasonable security measures in order to prevent data breaches. Can you elaborate? I was just Googling to try to find out what, under FTC, reasonable security measures mean. And I know that is a broad question, but yet—can you please, you know, share with us what reasonable security measures mean to the FTC? Because that is actually how you determine which cases to take or not take. Is that not really the crux of the issue?

Ms. RICH. Yes. So we—in reasonableness, we are referring to a bunch of factors which we have laid out again and again. The sensitivity and volume of information involved, you might want to have stronger security if you are talking about, you know, Social Security Numbers, than simply what, you know, size dress a person wears. The size and complexity of the data operations, a small company won't need to put as many protections in place if they have smaller data operations. And the cost of available tools to secure data and protect against known vulnerabilities. If there are not available tools out there that a company can learn about and use, it would not be—even if it could cause harm to consumers, it would not be reasonable to expect them to have known that.

Now, those are factors to look at, but we also really emphasize a process-based approach. Because if you undertake a responsible process, you should be able to get to the outcome of reasonable security. And also, process-based approach is tech neutral, so put somebody in charge. I was talking about this a bit earlier. Make somebody responsible. Somebody should be lying awake at night, worrying about this. You know, do a risk assessment. Put procedures in place to address those risks, focusing on such areas as training. Oversee your service provider. Periodically do evaluations and updates of your program. If you do those procedural things, and read all the information out there that provide guidance on what is reasonable security, you should be able to get to the reasonable security outcome.

Mrs. BROOKS. Thank you very much, and I look forward to also learning, in the future, Mr. Chairman, how the FTC—we are all focused on preventing the breach, enforcing if there has not been adequate security. I would love to know more about what we are doing to go after the hackers, and whether we never hear that we ever catch the hackers. Thank you, and I yield—

Mr. BURGESS. Chair thanks the gentlelady for that observation. Chair recognizes the ranking member of the full committee, Mr. Pallone. Five minutes for questions, please.

Mr. PALLONE. Thank you, Mr. Chairman. I wanted to ask Mr. Johnson these questions. I have a lot, so I am going to try to go through it quickly, if you could answer quickly. If this bill were to pass, Sections 201, 202, and 222 of the Communications Act, and all associated regulations, which include broad consumer privacy and data security protections, would no longer be in effect with respect to security of data in electronic form and breach notification.

So, Mr. Johnson, can you walk us through some examples of the types of consumer information that could have been required to be protected by Internet service providers under those sections? You know, first start, you know, could Internet browsing history have been protected?

Mr. JOHNSON. Well, I think that section, Section 222, has, for 18 years, been focused mostly on telephone communications. As of last month, the Commission's reclassification of broadband Internet access service expanded 222 to broadband providers, and there are presently no specific rules in place that pertain to the broadband service providers.

But I think that underscores the value of having public notice and comment rulemaking procedures to determine what exactly—what precisely that requires in—

Mr. PALLONE. So would you say that Internet browsing history could have been protected? Yes or no.

Mr. JOHNSON. It could be, potentially.

Mr. PALLONE. All right. How about the unique identifiers for wireless devices?

Mr. JOHNSON. By unique identifiers, could you tell me a little bit more?

Mr. PALLONE. Well, just tell me what you think would be protected, or could be protected—

Mr. JOHNSON. Well, what would—

Mr. PALLONE [continuing]. If it isn't at this point.

Mr. JOHNSON. The bill does transfer some of the protections for CPNI for call records data to the FTC, but what it doesn't transfer is a number of other things that pertain to the call service. And this is just on 222. For instance, how many calls a person makes in a day, what time they call, specific features of their call service, call waiting, caller ID. And, importantly, things that are not related to the telephone calls, but could be related to the service that they have, their financial status, whether they are low income. And that is just on 222. The bill also would remove all of the existing protections for cable and satellite and television viewing history, and related information.

Mr. PALLONE. So let me just ask a couple more. I know there are only 2 minutes. If the bill were enacted, the FCC would not be able to require Internet service providers to protect sensitive customer information?

Mr. JOHNSON. I think that is true. I think that is—

Mr. PALLONE. And the FCC would not be able to bring enforcement actions against Internet service providers that did not protect that information?

Mr. JOHNSON. I think that is correct.

Mr. PALLONE. And as you read this bill—and this is really the most important thing. As you read this bill, with regard to Internet service providers, would there be any protections for these types of customer info, beyond what is listed as personal information, in the definition section?

Mr. JOHNSON. I think there would not be beyond that definition, which is specific to financial harm and fraud—

Mr. PALLONE. All right.

Mr. JOHNSON [continuing]. And identity theft.

Mr. PALLONE. All right. Thanks so much.

Mr. BURGESS. Chair thanks the gentleman. Gentleman yields back his time. The Chair recognizes the gentleman from Mississippi, Mr. Harper. Five minutes for questions, please.

Mr. HARPER. Thank you, Mr. Chairman, and thank you both for being here. Ms. Rich, I just have a question. The legislative draft calls for uniform data breach and information security requirements housed at the FTC, including leveling the playing field by bringing telecommunication, cable, and satellite providers under the FTC regime. In your opinion, is the FTC the appropriate agency to oversee data security for the Internet, how shall we say, ecosystem?

Ms. RICH. We have been the lead agency on data security for now over 15 years, and we believe we should continue to provide that leadership, which is why we appreciated nonprofits being in the bill, and we appreciated carriers in the bill. The bill even, though, recognizes that others have a role to play. It allows the States to enforce, even if—as it preempts, it allows the States to enforce, and we would welcome that partnership with the States.

And as I mentioned before, we are—want to have common carrier authority so we can protect consumers, but we would be—we don't believe we should displace the FCC, or the majority of the Commission don't believe we should displace the FCC, so we would like to partner with them too in protecting consumers in the carrier area.

Mr. HARPER. Thank you, Ms. Rich, and I yield back the balance of my time.

Mr. BURGESS. Chair thanks the gentleman. Gentleman yields back. The Chair recognizes the gentleman from North Carolina, Mr. Butterfield. Five minutes for questions, please.

Mr. BUTTERFIELD. Thank you very much, Mr. Chairman. Thank you for holding today's hearing. Thank you to the witnesses for their testimony. This is absolutely an important issue, Mr. Chairman, that many members of this subcommittee are familiar with. You know, we have worked over the past few Congresses precisely on these concerns. As members of the subcommittee know, data breaches are occurring in alarming numbers all across the country. Just in North Carolina, our Attorney General estimates that about 6.2 million North Carolinians have been affected by data breaches since 2005, that is over the last 10 years, so I am glad we are addressing this issue today.

Our good friend and former chairman of the subcommittee, Mr. Rush, introduced a bipartisan bill entitled "The Data Accountability and Trust Act", and during my time as ranking member of this subcommittee, I worked very closely with then Chairwoman Bono, who I think I see here today, on the Secure and Fortify Electronic Data Act. There is plenty of precedent for finding bipartisan solutions on this subject.

There are some issues with the discussion draft before us today, and I encourage the majority to work with us so we can finally produce meaningful legislation that will give consumers the protections that they deserve, and businesses they—that—and businesses. They certainly need to grow and thrive.

Let me just address one or two questions to the witnesses. I may not take up the full 5 minutes, but I want to discuss the APA rule-making authority for just a moment. One important thing about that authority is that it allows an agency, such as yours, any agency with that authority, to implement a law over time. It is particularly important for laws concerning issues in which technical advances are common, and fairly quick, to be flexible and agile. As lawmakers, one thing we hate is having to revisit a law we recently passed because it is already out of date.

When Congress passed the Children's Online Privacy Law, it allowed the FTC to amend the definition of personal information through regular APA rulemaking procedures. Mr. Johnson, can you explain how the FCC has been able to ensure that Section 222 of the Act has stayed relevant at all times? How has Section 222 been updated to deal with problems over time, such as, most recently, when carriers were pre-installing software onto devices that had security flaws?

Mr. JOHNSON. Yes, sir, and I have already committed to providing a detailed timeline of FCC's history with 222, but I think that is a—your question is—gets right to the heart of the value of having the flexibility and the agility to adapt a statute to the changing technological landscape, and also the changing public expectations and Congressional expectations.

So since the—since Section 222 was enacted in 1996, entitled “Privacy of Consumer Information”, there have been a number of shifts. Obviously technologically, but also with regard to Congressional expectation. The first was in 1999, when, as part of the Wireless Communications Public Safety Act, the Commission added location information into the protected information under Section 222, and that is because 911 location accuracy is crucial.

There was just a—tragically, a woman in Georgia who made a 911 call on the border of a county line, and neither of the two call centers knew where she was, and it cost her her life, and this is something that we are trying to improve. And now, under a new rule that the Commission voted on earlier this year, hopefully soon the location accuracy will include being able to pinpoint where a person is, which room in a multi-story building they are in if they need help. But there are obviously incredibly specific privacy concerns that come with that type of location information.

Mr. BUTTERFIELD. Absolutely.

Mr. JOHNSON. So that is the type of thing that was added in 1999, and it has been improved over time, and—including the one that you mentioned, with regard to information collected on mobile devices in 2013.

Mr. JOHNSON. Right. All right. Let me go to Ms. Rich. Ms. Rich, your testimony called for FTC to be granted APA rulemaking authority to carry out the draft bill. Can you give us an example, beyond COPA, where such limited authority has allowed the FTC to deal with problems over time? And, finally, are there any instances where not having APA rulemaking authority inhibited the Commission's ability to effectively deal with problems?

Ms. RICH. The chief reason we want rulemaking authority in this area is, as you note, to allow us to adapt the consumer protections to make sure consumers are effectively protected, even as tech-

nology changes. So the Ranking Member mentioned geolocation as one type of information that we wouldn't have thought to protect not too many years ago, but another example is, we now know that the information that is collected through facial recognition is very sensitive, and we wouldn't have thought of that. It was only recently that it was recognized that Social Security Number alone could be used to perpetrate identity theft, particularly in the case of children, who don't have rich credit histories, and so it is very easy to take the Social Security Number, and pass it off as somebody else's.

So those are some examples of information we wouldn't have even known to protect a few years ago. And yes, we have a number of instances where we have used our rulemaking to not just adapt to change, but to respond when there were needless burdens on businesses in a law. We did that in CAN-SPAM. We used our rulemaking there. So there are a lot of examples.

Mr. BUTTERFIELD. Thank you very much, and thank you, Mr. Chairman, for not calling time prematurely on the witness. Thank you.

Mr. BURGESS. Chair thanks the gentleman. Chair recognizes the gentleman from Oklahoma, Mr. Mullin. Five minutes for questions, please.

Mr. MULLIN. Thank you, Mr. Chairman. Mr. Johnson, I would like to spend most of my time, if not all my time, visiting with you. Do you believe that a breach of information involving a number of someone's calls could maybe lead to theft or financial fraud? You mentioned about the cell phones a while ago. Do you see this could maybe cause a bigger problem down the road?

Mr. JOHNSON. As—let me make sure I understand your question. Could a breach of call data—

Mr. MULLIN. Of information. A breach of information involving the number of someone's call. Could this lead to a bigger problem?

Mr. JOHNSON. Let me not engage in hypotheticals, but I guess you could come up with some scenarios in which a breach of non-financial telecom information—

Mr. MULLIN. I mean, when you open that box, it leads down a road that is unknown. Like you said, you are being hypothetical on it.

Mr. JOHNSON. Um-hum.

Mr. MULLIN. And I think there is a lot of work that needs to be done. Now, obviously we want to protect the consumer. It is tragic what you brought up a while ago. I think most of us here read about that. We want to be able to protect people. I mean, I live way out in the middle of nowhere. My driveway is literally a mile long. The only way I get cell phone coverage is—

Mr. JOHNSON. Best way to—

Mr. MULLIN [continuing]. With the antenna that goes up my chimney, and I would want someone to be able to respond. There is no 911 address—

Mr. JOHNSON. Right.

Mr. MULLIN [continuing]. Where I live.

Mr. JOHNSON. Right.

Mr. MULLIN. And I get that. But at the same time, I don't want to open it up to exposing us to even a bigger risk. All of us live

in fear of fraud. The first time I had experience with that, someone went to school on my Social Security Number in California. At that time, I hadn't even been to California, and I got a phone call wanting to know what has happened. So it is something that we need to worry about.

Going on—you pointed out in your testimony, under the proposed bill, the FCC could lose rulemaking authority over data security. Has there been a—has the FCC effective—have been effective in using the authority to protect consumers in the 21st century?

Mr. JOHNSON. I would say, sir, that this will always be, as a cybersecurity—focus of my work is cybersecurity, and has been for years—this will always be a work in progress.

Mr. MULLIN. Right.

Mr. JOHNSON. We are not going to solve this problem. But I would say that I have—since I have been at the FCC, I have been very impressed with the clarity of the expectations that have developed, particularly on Section 222 of—

Mr. MULLIN. Well, do you know how many regulatory documents the FCC has published since '96?

Mr. JOHNSON. I don't know. You mean new rules?

Mr. MULLIN. Yes, new rules. Yes.

Mr. JOHNSON. We are committed to providing a full list of not just rules, but activities.

Mr. MULLIN. Well, according to the Federal Registry, the FCC has published nearly 14,000 rules since '96.

Mr. JOHNSON. Pertaining to—

Mr. MULLIN. No.

Mr. JOHNSON. Overall?

Mr. MULLIN. Overall. Do you know how many of those pertain to our 21st century security issues that we are having?

Mr. JOHNSON. I would have a ballpark, but it sounds like you—

Mr. MULLIN. Give me a ballpark.

Mr. JOHNSON [continuing]. An answer.

Mr. MULLIN. I don't, because—seriously, we did a lot of research trying to find it, and I really could not find it. In fact, my follow-up was, could you provide the information—

Mr. JOHNSON. There have been a few rulemakings and declaratory rulings on—specifically pertaining to 222, and we will get you those exactly.

Mr. MULLIN. Are they being implemented right now?

Mr. JOHNSON. Yes, sir.

Mr. MULLIN. Do you know how long it is going to take?

Mr. JOHNSON. Well, it is—I—it has been, and will always be, an ongoing process, but they are being implemented, and—

Mr. MULLIN. So it takes years to implement this?

Mr. JOHNSON. Well, I don't know if I would—I think the premise of your question may be that it finishes at some point, and the—

Mr. MULLIN. Technology doesn't finish—

Mr. JOHNSON. Right.

Mr. MULLIN [continuing]. And it seems like we are being very reactive, and we are not being proactive. We are responding to issues that happened years ago, and what we are trying to do is be in front of it.

Mr. JOHNSON. I understand.

Mr. MULLIN. And if we continue to be reactive, how are we ever going to get ahead of the game?

Mr. JOHNSON. Actually, I think you are absolutely right about the need to be proactive, and that is the value of having rule-making authority.

Mr. MULLIN. And I agree with that, but the problem that I have is, just recently, the FCC went all the way back to 1930. So how is that being proactive? I mean, we are wanting—you are wanting to keep the authority and have more authority. We are wanting to move forward. We are wanting to start being proactive, not reactive. You are making the argument that you want to keep it, but the recent actions of going all the way back to 1930 to a rule, how in the world, with today's technology, is that being proactive?

Mr. JOHNSON. You are referring to the open Internet—

Mr. MULLIN. Yes.

Mr. JOHNSON [continuing]. Order?

Mr. MULLIN. Of course I am.

Mr. JOHNSON. I will stay disciplined and remain in my lane on that. My focus is ensuring that the laws and policies are in place to ensure that telephone calls go through, that 911 calls have—

Mr. MULLIN. So let us finish on this, then. Do you really believe the FCC can continue to be proactive, or do you feel like you guys are being reactive?

Mr. JOHNSON. I think, actually, we are not only trying to be, but we are being proactive, and I can give you two examples. One is—

Mr. MULLIN. No, my time is out, but I am just going to tell you, from my opinion, it looks like we are being extremely reactive. Mr. Chairman, thank you. Mr. Johnson, thank you for your time. I yield back.

Mr. BURGESS. Chair thanks the gentleman. Gentleman yields back. Chair recognizes the gentleman from Illinois. Five minutes for questions, please, Mr. Kinzinger.

Mr. KINZINGER. Well, thank you, Mr. Chairman, and thank the witnesses for being here and spending a little time with us today, and thank the chairman for calling this hearing. I probably won't take all 5 minutes. I basically just have one question. I want to explore the issue of emails, and in this draft bill, email, data breach, et cetera. I know in Florida, their data breach and security notification law actually allows for email addresses, passwords, and—because in many cases many people have the same email and passwords into different sites, as well as, you know, they use it for login into something bigger.

Ms. Rich, in your testimony you note that within the draft legislation the definition of personal information does not protect some of the information which is currently protected under State law, I would guess that would be part of it with the email. Could you please expand on which elements that exist in the State law that would be most important for us to consider within a Federal statute, and would you include email and passwords in that?

Ms. RICH. I believe passwords are already in there in various capacities, but yes, the most important elements would be health, geolocation, and email—and communications. And device security.

And as I mentioned earlier, we have seen evidence that passport, driver's license, and other Government-issued numbers could be used, like Social Security Number, to perpetrate identity theft. So that is my list.

Mr. KINZINGER. So let us talk a little more about email address and password. Could an email address and password combination, could that lead to economic harm, and how could you see that happen? Is it more than just somebody has access to your email? Could that lead to bigger economic harm if that is stolen?

Ms. RICH. I can't spin out all the hypotheticals, but email address and password could get you into somebody's account, allow you to read their emails, allow you to communicate with perhaps accounts they have already set up with some sort of automated, you know, I know when I interact with accounts, I have often set it up, I know this is not a great practice—security practice, so that I can pretty quickly get on, it remembers me. So I think there are probably a lot of scenarios we can spin out with email and password.

Mr. KINZINGER. OK. And do you have any ideas as to, like, how do we reach that right balance of, you know, finding out what can be breached, and there is a problem, and also understand that we don't want to create legislation that is entirely too burdensome to people?

Ms. RICH. I think that the current draft already covers a nice broad class of information, and we are very complementary of the current draft. These were just a few additional items that we believe could cause consumer harm if they are intercepted by somebody else. And it is not an endless list. These are a few things we believe should be added.

Mr. KINZINGER. OK, great. And I will yield back a minute and 40 seconds, Mr. Chairman.

Mr. BURGESS. Thank you. Chair thanks the gentleman, gentleman yields back. Seeing there are no further members wishing to ask questions, I do want to thank both of you for your forbearance today. It has been very informative. Thank you for participating in today's hearing. This will conclude our first panel, and we will take a no-more-than-2-minute recess to allow the staff to set up for the second panel. Thank you, and this panel is dismissed.

[Recess.]

Mr. BURGESS. Mr. Leibowitz, we will begin with you. Five minutes for your opening statement, please.

STATEMENTS OF JON LEIBOWITZ, CO-CHAIRMAN, 21ST CENTURY PRIVACY COALITION; SARA CABLE, ASSISTANT ATTORNEY GENERAL, COMMONWEALTH OF MASSACHUSETTS; MALORY B. DUNCAN, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, NATIONAL RETAIL FEDERATION; LAURA MOY, SENIOR POLICY COUNSEL, OPEN TECHNOLOGY INSTITUTE, NEW AMERICA; AND Yael WEINMAN, VICE PRESIDENT FOR GLOBAL PRIVACY POLICY AND GENERAL COUNSEL, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

STATEMENT OF JON LEIBOWITZ

Mr. LEIBOWITZ. Thank you so much, Mr. Chairman. Chairman Burgess, Ranking Member Schakowsky, members of the panel, I want to thank you for inviting me to testify at this important hearing. Chairman Burgess, you and I worked together in the past on FTC related health care issues, and you bring a wealth of experience to your new role. And Ranking Member Schakowsky, you have been a leader on consumer protection issues, going back to your work at Illinois Public Action. Just as importantly, listening to this—to the panel and the questions, I can just tell that both of you are committed to finding practical solutions to real problems, which is why you will certainly develop many bipartisan initiatives going forward.

Along with Mary Bono, your former chairman—who is sitting over there, your former chairman—I serve as co-chair of the 21st Century Privacy Coalition. Our group is composed of the Nation's leading communications companies, which have a strong interest in modernizing data security laws to bolster consumers' trust in online services, and confidence in the privacy and data security of personal information. We are very supportive of the discussion draft legislation and what it seeks to accomplish.

Data security is an issue that I have cared deeply about for many years, going back to my time as a commissioner on the FTC. In fact, on behalf of the FTC, I testified before this subcommittee on this issue back in 2006. In testimony then, and it was testimony for a unanimous Federal Trade Commission, we urged Congress to "enact strong data security legislation that requires all businesses to safeguard sensitive personal information, and gives notice to consumers if there is a breach." And since then, as you know, the need for legislation has only grown dramatically.

You know all the statistics. Members have mentioned them. In 2014 we saw a number of data breaches. Just this morning in the Washington Post I read about a hack that may have exposed 11 million people, Primera customers, and their sensitive personal information. And when these breaches happen, they typically expose sensitive information. That is what all of the members had said in the first panel, how important that information is to consumers.

Data breaches resulting in the exposure of personal information can result in substantial harm to consumers. Companies that fail to take responsible measures to protect this information need to be held accountable. And that is why our coalition commends Representatives Blackburn and Welch, for releasing the Data Security and Breach Notification Act draft. The discussion draft contains

elements we believe are essential for effective data breach and data security legislation. Let me highlight just a few of them now.

First, the draft includes both breach notification standards and substantive data security requirements. While notifying consumers that a breach has occurred is important, it is ultimately of little value if companies are not required to put into place reasonable data security systems to protect consumers' sensitive information. In the first instance, these security requirements have to be strong, they should be clear, and they should be flexible to give consumers confidence, while giving companies a fair opportunity to comply with the law.

And some of this—I was listening to the back and forth with Mr. Pallone and the two witnesses earlier. It seems to me that some of the information they were talking about that might not be covered by the FCC could be covered, and would be covered—currently would be covered by the FTC in its UDAP statute, its Unfair and Deceptive Act or Practice statutes. We can talk about that more in the Q and A.

Second, the bill would replace the ever-changing patchwork of 47 different breach laws with a single Federal standard. A single Federal law reflects the reality that data is in cabin within individual States, but inherently moves in interstate commerce. Consumers in every part of the country are entitled to the same robust protections, and companies are entitled to a logical and coherent compliance regime, and only a bill with State law preemption can accomplish that.

Third, the draft smartly puts enforcement authority in the hands of America's top privacy cop, the Federal Trade Commission, while also empowering each State's Attorney General to enforce the Federal standard. The Federal Trade Commission, under both Democratic and Republican leadership, has, for many years, been our country's foremost protector of data security. The FTC has brought, and you heard this before from Jessica Rich, brought more than 50 data security enforcement actions in the last 10 years. And the draft would give the FTC more powerful tools, including fining authority, which it doesn't have now, to protect consumers and punish companies for inadequate protections. And moreover, by empowering State AGs to enforce the new Federal standard, the bill will ensure there are no gaps in enforcement. I think this bill is better for consumers than current law.

Mr. Chairman, given the President's strong endorsement for data breach legislation, as well as the growing support of the FTC, we believe you are poised to enact a law that provides strong protections for consumers, and holds companies to a single robust standard. In short, this measure would provide a practical solution to a real problem facing all Americans, and I commend members of this subcommittee for working on a bipartisan legislation.

With your permission, I ask that my full statement be put into the record. Thank you.

[The prepared statement of Mr. Leibowitz follows:]

Testimony of
The Honorable Jon Leibowitz
Co-Chairman, 21st Century Privacy Coalition
on
“Discussion Draft of the Data Security and Breach Notification Act of 2015”
before the
House Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade
March 18, 2015

Chairman Burgess, Ranking Member Schakowsky, other distinguished Members of the Subcommittee, thank you for inviting me to testify at this important hearing. Let me first congratulate Chairman Burgess on his new role. He and I have worked together in the past on FTC-related health care issues, and he brings a wealth of expertise and a commitment to consumer protection to this Subcommittee. And Ranking Member Schakowsky brings a deep devotion to consumer issues going back her work at Illinois Public Action. Just as importantly, both of you are committed to finding practical solutions to real problems, which is why you will almost certainly develop many bipartisan initiatives going forward.

My name is Jon Leibowitz and, along with former Representative Mary Bono, I serve as co-chair of the 21st Century Privacy Coalition. Our group is comprised of the nation's leading communications companies, which have a strong interest in modernizing privacy and data security laws to bolster consumers' trust in online services and confidence in the privacy and security of their personal information.

You do not have to be the former Chairman of the Federal Trade Commission ("FTC") to be aware of the explosion of data breaches over the past several years. While some of the high-profile breaches make headlines, others do not. Forty-three percent of respondents in an annual survey by the Ponemon Institute reported experiencing some sort of data breach in 2014, and the Bureau of Justice Statistics estimates that 7% of all U.S. residents ages 16 and older were victims of identity theft in 2012. Unauthorized access to personal information is a problem that affects businesses and consumers in all fifty states. In our increasingly interconnected nation and world,

few, if any, businesses operating online only serve customers in one state, and breaches thus have an impact that transcends state boundaries.

That is why our coalition commends Representatives Welch and Blackburn for releasing the Data Security and Breach Notification Act. We also commend the FTC for supporting data breach legislation for more than a decade, and the Obama Administration for reaffirming its commitment to data breach legislation earlier this year.

The United States needs a uniform, national framework that will provide consumers with clearer protections and businesses with greater certainty. Consumers in Texas deserve the same degree of protection as consumers in Illinois, and only Congress can ensure that all consumers enjoy the same robust protections. By the same token, consumers should be able to rely on the same protections regardless of whether their personal information is held by a communications provider, an edge provider engaged in online commercial transactions, or a brick and mortar retailer processing customer financial data over the Internet.

We believe that legislation should contain several key elements. First, it should require companies to employ reasonable data security protections. While we commend those who have focused more on data breach notification, companies should be utilizing reasonable, effective, and up-to-date information security procedures. But flexibility is critical – there is no one-size-fits-all set of standards that is appropriate for all companies. Hackers are constantly innovating, and companies therefore must have the ability to adapt and respond to the dynamic and constantly-shifting attack vectors and incursion strategies employed by data thieves.

We therefore support the inclusion of the flexible information security provision in the draft legislation, and appreciate the bill's implicit recognition that what constitutes reasonable security measures and practices will vary depending upon the company, the nature of its activities and the data it is safeguarding, the types of threats it faces, and the kinds of reasonable tools and practices available (and appropriate for the size and scale of the company) to meet those threats.

Second, while it is critical that consumers be notified in the case of a data breach that could result in identity theft or other financial harm, Congress should avoid requirements that produce over-notification. If consumers are constantly barraged with notifications about even minor breaches that do not involve financial harm, consumers are likely to ignore notifications, which means that they will not be paying attention when notified of significant breaches. As a result, we agree that notification should only occur if there is a reasonable risk of identity theft or other financial harm. The cyber hackers and data thieves behind the raft of high-profile breaches that we have seen over the past several years are seeking to harvest financial account information, credit card numbers, and identification data, and the draft correctly targets the data that poses the greatest risk of economic harm.

In addition, while consumers should be notified as quickly as possible, there are legitimate reasons why notification needs to be delayed. For example, delay may be necessary to permit law enforcement to conduct a criminal investigation, especially when it may be possible

to catch criminals in the act. Delay may also be necessary to permit a company to evaluate the scope of a breach, or mitigate its impact.

Third, a uniform national framework should be enforced by the Federal Trade Commission as well as State Attorneys General, and should preempt other laws and causes of action. Preemption will ensure the uniformity of the requirements that apply to every company, and the benefits that extend to every consumer. Having to comply with a patchwork of state requirements has created confusion and uneven protection even though a single breach rarely obeys state boundaries.

Moreover, we believe that national data security legislation should also preempt state common law. Once Congress enacts robust, national data security requirements, companies' focus should be on compliance with these requirements. The uniform national framework that is the objective of this legislation would be undermined if class actions can still be brought pursuant to state law. The result would be a continuation of the patchwork of state requirements that provide inconsistent protections for consumers across the United States today.

Duplicative or conflicting federal laws are no less harmful than duplicative or conflicting state laws. The Communications Act's data security requirements are a prime example. There is nothing "unique" about unauthorized access to consumer information held by communications providers. It is the same information as that held by many other players in the Internet ecosystem, which is why the same framework should apply the same law and the same standards to all entities that engage in online activities. The information protected under this legislation

should not be subject to different or duplicative legal regimes just because some companies have historically been subject to certain requirements and others have not. The national policy enacted by this bill should put all companies on equal footing with respect to their data security and breach notification obligations.

The FTC is undoubtedly the preeminent federal agency policing data security. The FTC has a long and extraordinary history of enforcement experience, having brought more than fifty data security cases, over a hundred Do Not Call cases, and numerous other cases for various types of privacy violations. The FTC's Consumer Protection Bureau has a staff of dedicated professionals with decades of experience evaluating the reasonableness of companies' data security practices. And with this legislation, the FTC will gain a powerful new tool to use against companies that do not protect data security—fining authority. The agency currently lacks fining authority for unfair or deceptive acts or practices violations, except against companies that are already under an FTC order.

The Federal Trade Commission should be fully empowered to penalize companies that violate federal data security requirements. Subject to intervention by the FTC, State Attorneys General should also be able to go into court to enforce the new law's requirements.

Mr. Chairman, thank you for holding this hearing today. Our coalition commends the Subcommittee for a draft bill that would create a comprehensive, uniform national data security framework that includes the elements we have referenced in our testimony.

We look forward to working with this Subcommittee as it moves forward with legislation. Given the bipartisan congressional support for data breach legislation as well as support from the President and the FTC, we believe that Congress is poised to enact legislation that better protects consumers, and avoids the pitfalls inherent in today's patchwork of conflicting laws and requirements.

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

Mr. BURGESS. Without objection, so ordered.

Ms. Cable, welcome to the subcommittee. You are recognized. 5 minutes for your opening statement, please.

STATEMENT OF SARA CABLE

Ms. CABLE. Thank you. Good morning, Chairman Burgess, Ranking Member Schakowsky, distinguished members of the subcommittee. Thank you for inviting me here today to testify. My name is Sara Cable, and I am an Assistant Attorney General with the Office of the Massachusetts Attorney General, Maura Healey, and I am here today on behalf of my office to present some of our concerns with the bill.

My comments today are informed by my office's experience enforcing Massachusetts data security and breach laws, which are regarded as among the strongest in the country. My office works hard to use those laws to protect our residents, and we believe that our consumers are better protected as a result. We are encouraged that the subcommittee recognizes a critical necessity of data security and breach protections. We share this goal. This is our most sensitive information. Yours, mine, our children, our parents, our co-workers, our friends. We are all impacted, and we all deserve robust protections.

We understand Federal standardization is the thrust of this bill. We do, however, have serious concerns that the standards set by this bill are too low, preempt too much, and hamstring the ability of my office, and that of the other Attorney General offices across the country, to continue our important work of protecting our consumers. It is our concern that this bill would—as drafted would set aside the robust consumer protections that already exist in Massachusetts and many other States, and replace them with weaker protections at a time when strong protections are imperative.

My first point focuses on the bill's proposed data security standard. We agree strong data security standards are essential. This is how breaches are prevented. This is how the whole business of providing notice of breaches can be prevented. The bill would require "reasonable security measures and practices." Our concern, however, is that it does not specify or delineate precisely what practices or measures are required. It may be true reasonableness is a useful standard in general, but it—standing alone, it is not particularly useful when trying to understand what actual practices and measures are required.

We think that the only way reasonable can be determined under the bill as drafted will be through piecemeal protracted litigation, and the standard will differ from case to case and company to company. It will cause needless confusion, expense, and risk for companies, who are forced to guess what measures and practices will ultimately be considered by—considered reasonable.

We think Massachusetts has the better approach. It has in place data security regulations that are tech neutral, process-oriented, and, importantly, describe the basic minimum components of a reasonable data security program. Some of those components are—you have heard them from the FTC earlier today, conducting a risk assessment, developing, implementing, and maintaining a written information security program, establishing computer security con-

trols, and many others. The Massachusetts regulations are consistent with those currently in place under Gramm-Leach-Bliley and HIPAA. We believe that they provide stronger protections to our consumers. Our view is that the bill as drafted would erase these strong protections, and, we believe, would ultimately be harmful to consumers.

My second point concerns the scope of the bill's preemption. Put simply, we think it is too broad. It would restrict my office's ability to enforce our own consumer protection laws. It would prevent innovative States from legislating in this field in response to purely local concerns, for example, a breach involving a Massachusetts company and Massachusetts residents only. Under my interpretation, I think the bill might even go further, and it might possibly restrict States from enforcing, for example, criminal laws relating to the unauthorized access of electronic communications. It might possibly also preempt a State's ability to enforce the security obligations under HIPAA, an enforcement power given to the States under the High Tech Act. These laws, and others, relate to the issue of unauthorized access to data in electronic form, and under the current language of the bill, we believe our State's ability to enforce those laws would be preempted.

Finally, the bill hamstringing my office's ability to protect Massachusetts consumers. Currently, under Mass law, we get notice of any breach involving one or more Massachusetts residents. From January 2008 through July 31, 2014 Massachusetts has received notice of over 8,600 breaches, impacting over five million Massachusetts consumers. That is in Massachusetts alone. Under this bill, we would receive none of those notices. We believe this is a critical omission in the bill. It restricts our ability to enforce the requirements of the bill, and we believe ultimately it will make our job of protecting our consumers a lot more difficult.

And with that, I thank the subcommittee for their efforts and for inviting me today. Thank you very much.

[The prepared statement of Ms. Cable follows:]

SUMMARY OF THE TESTIMONY OF
SARA CABLE, ASSISTANT ATTORNEY GENERAL
OFFICE OF ATTORNEY GENERAL MAURA HEALEY
COMMONWEALTH OF MASSACHUSETTS

BEFORE THE

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

HEARING ON

THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2015

MARCH 18, 2015

Chairman Burgess, Ranking Member Schakowsky, members of the Subcommittee, thank you for inviting me to testify today regarding the proposed Data Security and Breach Notification Act of 2015 (the "Bill"). I am here on behalf of the Office of Attorney General Maura Healey to present the concerns of my Office with regard to the Bill. My comments are informed by my experience enforcing Massachusetts' data security breach notification law (Mass. Gen. Law ch. 93H), the Massachusetts data security regulations (Title 201 of the Code of Massachusetts Regulations, section 17.00 *et seq.*), and the Massachusetts data disposal law (Mass. Gen. Law ch. 93I). These laws are regarded as among the strongest in the country.

While I am cognizant of the business community's concerns regarding compliance with myriad state security breach notification regimes, I am here today to address serious reservations with the Bill, which I believe represents a significant retraction of existing protections for consumers at a time when such protections are imperative. The principal concerns with the Bill that I wish to highlight are as follows:

1. The proposed preemption of state law undercuts existing consumer protections and is overly broad.
2. Minimum data security standards are important and necessary, but the proposed standards leave consumers' data vulnerable.
3. The Bill fails to require notice that will ensure meaningful enforcement.
4. The Bill infringes on the States' consumer protection enforcement authority.
5. The penalties proposed by the Bill are insufficient, and leave consumers without a remedy.
6. The Bill's data breach notice obligations lack many key safeguards.

I appreciate this opportunity to convey to the Subcommittee our serious concerns regarding the Bill. Please do not hesitate to contact us for any additional information, clarity, or with questions you may have as you proceed.



MAURA HEALEY
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

TEL: (617) 727-2200
www.mass.gov/ago

March 17, 2015

The Honorable Michael C. Burgess M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

Re: *The Data Security and Breach Notification Act of 2015*

Dear Chairman Burgess and Ranking Member Schakowsky:

We write to address the discussion draft bill entitled the Data Security and Breach Notification Act of 2015 (the "Bill"), dated March 12, 2015, which seeks to establish federal standards concerning data security and data breach notification obligations. We appreciate that the Committee recognizes the importance of strong data security protections and breach disclosure obligations to protect consumers and preserve consumer confidence in the market. Moreover, we are cognizant of the business community's concerns regarding compliance with myriad state security breach notification regimes.

Nonetheless, we write to express serious reservations with the Bill, which in our view represents an unnecessary retraction of existing protections for consumers at a time when such protections are imperative. Our concerns are informed by this Office's experience enforcing Massachusetts' data security breach notification law (Mass. Gen. Law ch. 93H, attached as Exhibit 1), data security regulations (Title 201 of the Code of Massachusetts Regulations ("CMR"), section 17.00 *et seq.*, attached as Exhibit 2), and data disposal law (Mass. Gen. Law ch. 93I, attached as Exhibit 3). Together, these laws and regulations – which are enforced by this Office through the Massachusetts Consumer Protection Act¹ – require entities that own or license "personal information"² of Massachusetts residents to develop, implement, and maintain

¹ Mass Gen. Law ch. 93A.

² In Massachusetts, "personal information" is defined by statute to mean a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security

minimum security procedures and policies consistent with industry standards to safeguard such information (whether in paper or electronic form) from anticipated threats or hazards and from unauthorized access or use.³ Massachusetts law also obligates entities to provide prompt notice to affected residents and state agencies in the event of a breach of security or compromise of that information.⁴ These laws and regulations protect consumers from identity theft and fraud, and concomitantly, instill consumer confidence in the commercial collection and use of their personal information.

From January 1, 2008 through July 31, 2014, this Office received notice pursuant to Mass. Gen. Law ch. 93H, section 3 of over 8,665 security breaches, affecting nearly 5 million Massachusetts residents. To the extent any of those breaches resulted in enforcement actions by this Office (a very small percentage), the circumstances reflected gross failures to implement or maintain basic security practices, unreasonable delays in providing notice of the breach, or other egregious conduct that raised real risks of resulting consumer harm. As a result, this Office has an informed and comprehensive view into the nature, extent, and frequency of data breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

Accordingly, this Office is uniquely positioned to highlight some of the potential problems with the Bill. Our principal concerns are as follows:

I. The Bill's proposed preemption of state law undercuts existing consumer protections and is overly broad.

Although the stated purpose of the Bill is to "protect consumers from identity theft, economic loss or economic harm, and financial fraud," the Bill would preempt Massachusetts' data security/breach law to the extent they relate to data in electronic form, and replace it with weaker protections. In addition, the Bill would preempt other state laws that protect "data in electronic form" from unauthorized access (including, among others, laws that criminalize the interception of wire communications (Mass Gen. Law c. 272, § 99(C)) or require the confidentiality of medical records and mental health records (Mass Gen. Law c. 111, § 70E(b), and c. 123, § 36)). It is also in conflict with, and would appear to potentially preempt, the enforcement authority given to the States under other federal laws relating to the security of electronic data (including, for example, the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 1320d-5(d))). Such sweeping preemption is harmful to consumers, and restricts innovative States from responding to and protecting their residents from emerging threats to the privacy and security of their data. The Bill should at least preserve the current level of protections enjoyed by consumers and the enforcement powers of the state Attorneys General to avoid a national downward harmonization of security and breach standards, and an associated drop in consumer confidence in the marketplace. The Bill will not only fail to

number; or (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. See Mass Gen. Law ch. 93H, §1.

³ See Mass Gen. Law ch. 93I and 201 CMR 17.00 *et seq.*

⁴ See Mass Gen. Law ch. 93H.

maintain consumer confidence in the marketplace, but will scale back the protections consumers currently enjoy.

II. Minimum data security standards are important and necessary, but the proposed standards leave consumers' data vulnerable.

We agree that establishing minimum data security standards is important and necessary. Massachusetts has had robust minimum data security regulations in place since 2010 in the form of data security regulations (201 CMR 17.00 *et seq.*) and data disposal law (Mass Gen. Law ch. 93I). The flexible standards established by Massachusetts represent the leading information security framework in the nation, and are the standards to which all commercial entities aspire.⁵ We are concerned the Bill will lower the bar already set by Massachusetts and other existing federal data security regulations,⁶ and will weaken consumers' confidence in the security of their personal information in commerce. Specifically, the Bill fails to articulate the minimum data security standards that would constitute the required "reasonable security measures and practices." As a result, the Bill would result in the retroactive establishment of data security standards through protracted litigation and piecemeal judicial interpretation. To ensure that the data security obligations are sufficiently robust, defined, and responsive to changing threats and technologies, the Bill should establish minimum data security standards, modeled after those in place in Massachusetts and under existing federal law.

III. The Bill fails to require notice that will ensure meaningful enforcement.

While the Bill's requirement of notice of a breach to the Federal Trade Commission is an important first step for enforcement of the Bill's requirements, it is not by itself enough. Recent breaches reported in the media underscore the necessary role played by the state Attorneys General in enforcing data breach and data security requirements. The absence of a requirement to provide notice to state Attorneys General of data breaches – even for those breaches that impact a significant number of their residents – frustrates their ability to protect their residents. Further, the threshold for providing notice to the FTC may be set too high. In Massachusetts, the vast majority (approximately 97%) of the 2,314 data breaches reported in 2013 involved fewer than 10,000 persons; each of these breaches affected, on average, 74 persons. Assuming these statistics are consistent nationally, the Bill would create an enforcement "blind spot" for both

⁵ Similar to existing federal standards applicable to financial institutions (*see* 16 C.F.R. Part 314) and entities covered under HIPAA (*see e.g.* 45 CFR Subpart C of Part 164), Massachusetts requires entities to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information (201 CMR 17.03(2)(b)); develop, implement and maintain a "written comprehensive information security program" containing physical, administrative and technical safeguards necessary to protect personal information from those risks (201 CMR 17.03); take reasonable steps to oversee third parties handling personal information (201 CMR 17.03(2)(f)); and securely dispose of personal information (Mass Gen. Law ch. 93I). Cognizant of the particular risks associated with electronic data, Massachusetts also requires entities, among other things, to establish and maintain a technically-feasible computer security system (201 CMR 17.04); and to encrypt personal information sent over public networks or wirelessly, or stored on laptops and portable devices (201 CMR 17.04(3), (5)).

⁶ *See, e.g.*, 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information); 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information); 16 CFR Part 682 (Proper Disposal of Consumer Information); and 201 CMR 17.00 *et seq.* (Standards for the Protection of Personal Information of Residents of the Commonwealth).

state and federal regulators, who would not receive notice of the vast majority of data breaches that occur. To ensure effective enforcement of the Bill, the Bill should require prompt notice of breaches to the FTC and also to the state Attorneys General in cases where their State's residents are impacted.

IV. The Bill infringes on the States' consumer protection enforcement authority.

While the Bill gives the state Attorneys General the option of bringing a civil action as *parens patriae* in U.S. district court, it requires the State to first notify the FTC, and to abstain from that action if the FTC initiates the action first. Such requirements infringe on the enforcement prerogatives of the state Attorneys General by injecting unnecessary delay and costs, and unnecessarily complicating their efforts to enforce their respective consumer protection laws. Numerous federal laws illustrate that dual federal/state enforcement coordination of consumer protection laws is both possible and effective, including for example: the Federal Trade Commission Act (15 U.S.C. § 45(a)(1) and its numerous State counterparts (*see, e.g.* Mass Gen. Law ch. 93A), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and the Health Information Technology for Clinical and Economic Health (HITECH) Act (42 U.S.C. § 17930 *et seq.*). To ensure meaningful protections for consumers, the Bill should likewise establish a dual federal/state enforcement framework that respects – not constricts – the enforcement prerogative of the States.

V. The penalties proposed by the Bill are insufficient, and leave consumers without a remedy.

The Bill limits the state Attorneys General to civil penalties of up to \$11,000 for each day per violation of the Bill's information security requirements, and up to \$11,000 per violation of the Bill's breach notice requirements, capped at a total liability of \$2.5 million, and based on "penalty factors" that do not expressly take into account consumer harm or the need to deter future violations. Given the massive scope of recently-reported breaches affecting some of the largest companies in the country, a civil penalty cap of \$2.5 million may be an insufficient deterrent, and could be treated as a cost of doing business. Moreover, the Bill does not authorize the state Attorneys General to recover consumer restitution, and further does not provide for a private cause of action. Thus, a consumer who suffers loss due to a data breach effectively has no remedy under this Bill. The Bill should instead retain the existing discretion of state Attorneys General and the FTC to seek both civil penalties and consumer restitution at levels sufficient to penalize and deter the conduct at issue and make consumers whole, and further provide a private right of action.

VI. The Bill's data breach notice obligations lack many key safeguards.

Requiring prompt notice to consumers affected by a breach and to state regulators serves important ends, including alerting consumers to the fact that their personal information may be at risk, educating the market as to existing or emerging security threats, and providing incentives for improving security practices to prevent breaches. The data breach notice standards proposed by the Bill fall short for a number of reasons.

First, the Bill allows entities to delay notice without regard to the risks faced by consumers. By requiring notice only when the entity both “discovers” a “breach of security” and “determines” that a “reasonable risk of” identity theft, economic loss or harm, or financial fraud has resulted or will result, the Bill creates a disincentive for an entity to monitor their systems for potential compromises or vulnerabilities, an outcome directly at odds with the Bill’s stated purposes. Once “discovered,” the Bill would further grant a covered entity an unspecified (and unlimited) period of time to “tak[e] the necessary measures” to “determine the scope of the breach of security and restore the reasonable integrity, security, and confidentiality” of its data system. This creates opportunities for delay that would undermine the force of the proposed thirty (30) day notification deadline, and which may subject consumers to unnecessary risk. If preventing identity theft is the goal, notice should be issued in time for consumers to protect themselves, even if the breached entity has not completed its investigation or is still in the process of restoring its systems.

Second, the Bill fails to require notice in cases where identity theft is a real risk, such as when personal information is accessed or acquired with authorization (e.g. by an authorized employee) but used for unauthorized purposes. Additionally, the Bill does not provide for notice in cases where encrypted personal information – and information allowing for the decryption of that information – are both compromised in the breach.

Third, because notice obligation under the Bill turns on the manner in which a covered entity deals with the personal information, rather than its legal relationship to it,⁷ notice could be delayed or avoided as a result of disputes between covered entities as to which is the “third-party entity” and which is the covered entity responsible for notice. It may also result in consumer confusion insofar as consumers may receive notice from an entity with which they have not had direct dealings. To avoid such results, the Bill should follow Massachusetts’ lead and impose the consumer notification duty on the entity that “owns or licenses” the breached personal information. In turn, entities that “maintain or store” the breached personal information should be obligated to promptly notify the owner or licensor. See Mass Gen. Law ch. 93H, §§ 3(a), (b).

Finally, the content and form of the required consumer notice lacks several key safeguards. The Bill does not require the notice to contain information as to how a consumer may protect him or herself and instead, directs the consumer to the FTC for more information. The Bill should require the consumer notice to contain the information necessary for the consumer to protect him/herself from identity theft.⁸ In cases where “substitute notice” is

⁷ The Bill imposes the consumer notice obligation on “a covered entity that uses, accesses, transmits, stores, disposes of, or collects” personal information (section 3(a)(1)), but not on the covered entity that “store[s], processe[s], or maintain[s]” personal information” for a covered entity. This “third-party entity” would “ha[ve] no other notification obligations” than to notify the covered entity for whom it stores, processes, or maintains the personal information (section 3(b)(1)(A)).

⁸ Such information should include, for example, information concerning the availability of security freezes, the importance of filing and obtaining a police report (information required under Mass Gen. Law ch. 93H, § 3), the availability of fraud alerts, the importance of monitoring one’s credit reports, and other information about the breach that would allow the consumer to fairly assess their risk and protect themselves.

authorized, the entity should be required to make a media posting sufficient to constitute legal notice of the breach.⁹

We appreciate this opportunity to convey our serious concerns regarding the Bill to the Subcommittee. Please do not hesitate to contact us for any additional detail, clarity or with questions you may have. We are happy to provide you with any information you may need or to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws.



Jonathan B. Miller
Chief, Public Protection and Advocacy Bureau

Sara Cable
Assistant Attorney General
Consumer Protection Division

Office of Attorney General Maura Healey
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108
(617) 727-2200

⁹ See, e.g. Mass Gen. Law ch. 93H, § 1 (requiring as one component of substitute notice “publication in or broadcast through media or medium that provides notice throughout the commonwealth [of Massachusetts]”).

EXHIBIT 1

§ 1. Definitions, MA ST 93H § 1

Massachusetts General Laws Annotated
 Part I. Administration of the Government (Ch. 1-182)
 Title XV. Regulation of Trade (Ch. 93-110h)
 Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 1

§ 1. Definitions

Effective: October 31, 2007
 Currentness

(a) As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:--

“Agency”, any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

“Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

“Data” any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Electronic”, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

“Encrypted” transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.

“Notice” shall include:--

(i) written notice;

(ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G; or

(iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

“Person”, a natural person, corporation, association, partnership or other legal entity.

§ 1. Definitions, MA ST 93H § 1

"Personal information" a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

- (a) Social Security number;
- (b) driver's license number or state-issued identification card number; or
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Substitute notice", shall consist of all of the following:--

- (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;
 - (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and
 - (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.
- (b) The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted", as used in this chapter, to reflect applicable technological advancements.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)

M.G.L.A. 93H § 1, MA ST 93H § 1

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

Massachusetts General Laws Annotated Part I. Administration of the Government (Ch. 1-182) Title XV. Regulation of Trade (Ch. 93-110h) Chapter 93H. Security Breaches (Refs & Annos)
--

M.G.L.A. 93H § 2

§ 2. Regulations to safeguard personal information of commonwealth residents

Effective: October 31, 2007
 Currentness

(a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

(b) The supervisor of records, with the advice and consent of the information technology division to the extent of its jurisdiction to set information technology standards under paragraph (d) of section 4A of chapter 7, shall establish rules or regulations designed to safeguard the personal information of residents of the commonwealth that is owned or licensed. Such rules or regulations shall be applicable to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court, and the rules and regulations shall take into account the size, scope and type of services provided thereby, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

(c) The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor shall adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

§ 2. Regulations to safeguard personal information of..., MA ST 93H § 2

Notes of Decisions (1)

M.G.L.A. 93H § 2, MA ST 93H § 2

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

§ 3. Duty to report known security breach or unauthorized use of..., MA ST 93H § 3

Massachusetts General Laws Annotated
 Part I. Administration of the Government (Ch. 1-182)
 Title XV. Regulation of Trade (Ch. 93-110h)
 Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 3

§ 3. Duty to report known security breach or unauthorized use of personal information

Effective: October 31, 2007

Currentness

(a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor of such information. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use. (b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) ¹ If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or

§ 3. Duty to report known security breach or unauthorized use of..., MA ST 93H § 3

use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)**Footnotes**

1 So in original.

M.G.L.A. 93H § 3, MA ST 93H § 3

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

§ 4. Delay in notice when notice would impede criminal..., MA ST 93H § 4

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 4

§ 4. Delay in notice when notice would impede criminal investigation; cooperation with law enforcement

Effective: October 31, 2007

Currentness

Notwithstanding section 3, notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)

M.G.L.A. 93H § 4, MA ST 93H § 4

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

§ 5. Applicability of other state and federal laws, MA ST 93H § 5

Massachusetts General Laws Annotated Part I. Administration of the Government (Ch. 1-182) Title XV. Regulation of Trade (Ch. 93-110h) Chapter 93H. Security Breaches (Refs & Annos)
--

M.G.L.A. 93H § 5**§ 5. Applicability of other state and federal laws**

Effective: October 31, 2007
Currentness

This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

M.G.L.A. 93H § 5, MA ST 93H § 5

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

§ 6. Enforcement of chapter, MA ST 93H § 6

<p>Massachusetts General Laws Annotated Part I. Administration of the Government (Ch. 1-182) Title XV. Regulation of Trade (Ch. 93-110h) Chapter 93H. Security Breaches (Refs & Annos)</p>

M.G.L.A. 93H § 6

§ 6. Enforcement of chapter

Effective: October 31, 2007
Currentness

The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

M.G.L.A. 93H § 6, MA ST 93H § 6

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT 2

17.01: Purpose and Scope, 201 MA ADC 17.01

Code of Massachusetts Regulations Currentness**Title 201: Office of Consumer Affairs and Business Regulation****Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
(Refs & Annos)****201 CMR 17.01****17.01: Purpose and Scope**

(1) Purpose. 201 CMR 17.00 implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. 201 CMR 17.00 establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of 201 CMR 17.00 is to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope. 201 CMR 17.00 applies to all persons that own or license personal information about a resident of the Commonwealth.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.01, 201 MA ADC 17.01

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Code of Massachusetts Regulations Currentness
 Title 201: Office of Consumer Affairs and Business Regulation
 Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
 (Refs & Annos)

201 CMR 17.02

17.02: Definitions

The following words as used in 201 CMR 17.00 shall, unless the context requires otherwise, have the following meanings:

Breach of Security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or Licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal Information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

- (a) Social Security number;
- (b) driver's license number or state-issued identification card number; or
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service Provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to 201 CMR 17.00.

17.02: Definitions, 201 MA ADC 17.02

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.02, 201 MA ADC 17.02

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Code of Massachusetts Regulations Currentness
 Title 201: Office of Consumer Affairs and Business Regulation
 Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
 (Refs & Annos)

201 CMR 17.03

17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

- (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
- (b) the amount of resources available to such person;
- (c) the amount of stored data; and
- (d) the need for security and confidentiality of both consumer and employee information.

The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to maintain the comprehensive information security program;
- (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
 - 1. ongoing employee (including temporary and contract employee) training;
 - 2. employee compliance with policies and procedures; and
 - 3. means for detecting and preventing security system failures.
- (c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

17.03: Duty to Protect and Standards for Protecting Personal..., 201 MA ADC 17.03

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2. even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.03, 201 MA ADC 17.03

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Code of Massachusetts Regulations Currentness

Title 201: Office of Consumer Affairs and Business Regulation

Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
(Refs & Annos)

201 CMR 17.04

17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

- (1) Secure user authentication protocols including:
 - (a) control of user IDs and other identifiers;
 - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - (d) restricting access to active users and active user accounts only; and
 - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:
 - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- (5) Encryption of all personal information stored on laptops or other portable devices;

17.04: Computer System Security Requirements, 201 MA ADC 17.04

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.04, 201 MA ADC 17.04

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

17.05: Compliance Deadline, 201 MA ADC 17.05

<p>Code of Massachusetts Regulations Currentness Title 201: Office of Consumer Affairs and Business Regulation Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth (Refs & Annos)</p>

201 CMR 17.05

17.05: Compliance Deadline

(1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.05, 201 MA ADC 17.05

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT 3

§ 1. Definitions, MA ST 93I § 1

Massachusetts General Laws Annotated
 Part I. Administration of the Government (Ch. 1-182)
 Title XV. Regulation of Trade (Ch. 93-110h)
 Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 1

§ 1. Definitions

Effective: February 3, 2008
 Currentness

As used in this chapter the following words shall, unless the context clearly requires otherwise, have the following meanings:--

"Agency", any county, city, town, or constitutional office or any agency thereof, including but not limited to, any department, division, bureau, board, commission or committee thereof, or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction.

"Data subject", an individual to whom personal information refers.

"Person", a natural person, corporation, association, partnership or other legal entity.

"Personal information", a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident:--

- (a) Social Security number;
- (b) driver's license number or Massachusetts identification card number;
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or
- (d) a biometric indicator.

Credits

Added by St.2007, c. 82, § 17, eff. Feb. 3, 2008.

M.G.L.A. 93I § 1, MA ST 93I § 1

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

§ 2. Standards for disposal of records containing personal..., MA ST 93I § 2

Massachusetts General Laws Annotated
 Part I. Administration of the Government (Ch. 1-182)
 Title XV. Regulation of Trade (Ch. 93-110h)
 Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 2

§ 2. Standards for disposal of records containing personal information; disposal by third party; enforcement

Effective: February 3, 2008
 Currentness

When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than \$100 per data subject affected, provided said fine shall not exceed \$50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

Credits

Added by St.2007, c. 82, § 17, eff. Feb. 3, 2008.

M.G.L.A. 93I § 2, MA ST 93I § 2

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

§ 3. Enforcement, MA ST 93I § 3

<p>Massachusetts General Laws Annotated</p> <p>Part I. Administration of the Government (Ch. 1-182)</p> <p>Title XV. Regulation of Trade (Ch. 93-110h)</p> <p>Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)</p>

M.G.L.A. 93I § 3

§ 3. Enforcement

Effective: February 3, 2008
Currentness

The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

Credits

Added by St.2007, c. 82, § 17, eff. Feb. 3, 2008.

M.G.L.A. 93I § 3, MA ST 93I § 3

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

Mr. BURGESS. The Chair thanks the gentlelady.

Mr. Duncan, welcome to the subcommittee. You are recognized 5 minutes for the purpose of an opening statement.

STATEMENT OF MALLORY B. DUNCAN

Mr. DUNCAN. Thank you, Dr. Burgess, Ranking Member Schakowsky, members of the committee for inviting us here today, and particularly Congressmen Blackburn and Welch for their efforts to produce this draft legislation. Thank you too for the courtesy and consideration you and your staffs have shown to us and our members over the past many months. The result of those discussions, and undoubtedly many more, is a working draft that is significantly better than introducing—legislation introduced in prior Congresses. We look forward to continue working with you to help turn the draft into a legislative product that will provide increased security and protection for consumers, ameliorate burdens on business, and establish meaningful and reasonable standards for all.

I would like to set out three or four principles that have guided our work. Number one, breaches affect everyone. Every entity that has a significant breach of sensitive data should have an obligation to make that fact publicly known. Public notice serves two goals. First, it provides consumers with information they might be able to use to better protect themselves from identity theft. Second, the fear of public notice strongly incentivizes companies to improve their security. Both goals are important. Enacting legislation that exempts some entities from public notice, or that perpetuates notice holes that would allow companies to hide breaches undermines both.

Two, if one is a mid-sized regional company, or an e-commerce startup struggling with the consequences of a breach, the existing morass of inconsistent laws are little more than traps for the unwary. We need Federal preemption that works.

Three, if we are going to preempt the State laws, we owe it to the States, and to their citizens, not to adopt a weak law. We should seek legislation that reflects a strong consensus of the State laws and carefully strengthen them where doing so supports the other two principles.

And four, if we are to specifically adopt data security standards, they should not be defined technical standards, and they must be comprehensible and actionable from the perspective of the companies against whom they will apply.

With those principles in mind, I would like to address a few areas of the draft. One, there is not good reason why a breach law should apply a high standard for reporting against some companies, such as retailers, restaurants, dry cleaners, and other small businesses, while requiring little or no notice from some of the biggest firms in America holding the same sensitive data, be they cloud services like Apple, or payment processors like Heartline when they suffer a breach. Not only does the draft excuse them from general public notice, undermining security incentives, the draft allows big businesses to shift liability for their breaches onto smaller business. This is worse than what exists under the State laws. It must be fixed.

Two, preemption. In general, the preemption language in the draft is much better than in previous Congresses' bills. If the notice holes are filled, it could replace the conflicting welter of State requirements with a single strong law. The one area for concern is the clause that specifically excludes some laws from preemption. Federal jurisprudence suggests that when that is done, the entire preemption clause could be placed in jeopardy.

Three, there are portions of the draft that are inconsistent with the considered strong consensus of State laws. For example, we know of no State law that expressly exempts communication service providers, and that would allow them, even when they know they have a serious breach, to get away with providing no notice to anyone at all. That is a notice hold you could drive a truck through.

Finally, as to data security, when the FTC applies generalized standards to businesses, such as unfairness or deception, as—or, as should be proposed here, reasonable security standards, they are enforced under Section 5 of the FTC Act, which calls for a cease and desist order before penalties can be imposed. The law allows businesses to understand what is intended by the vague standards before they are made subject to massive penalties.

While going directly to damages might be appropriate for an objective on/off requirement, like giving notice within 30 days, it does not make sense when the legal requirement is simply to do something reasonable, or not to be unfair. That is the way the Commission has worked very effectively for over 100 years. Congress should not leave companies subject to fines for practices they could not know in advance, or unreasonable in the eyes of the FTC. That must be remedied.

Thank you for the opportunity to speak today. We look forward to working with you to craft a strong, effective, and fair law.

[The prepared statement of Mr. Duncan follows:]



TESTIMONY OF

MALLORY B. DUNCAN

GENERAL COUNSEL AND SENIOR VICE PRESIDENT,
NATIONAL RETAIL FEDERATION

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

HEARING ON

“DISCUSSION DRAFT OF H.R. ____, DATA SECURITY AND
BREACH NOTIFICATION ACT OF 2015”

MARCH 18, 2015

National Retail Federation
1101 New York Avenue, NW
Suite 1200
Washington, DC 20005
(202) 626-8126
www.nrf.com

TESTIMONY OF

MALLORY B. DUNCAN

GENERAL COUNSEL AND SENIOR VICE PRESIDENT,
NATIONAL RETAIL FEDERATION

Chairman Burgess, Ranking Member Schakowsky, and members of the Subcommittee, on behalf of the National Retail Federation (NRF), I want to thank you for giving us the opportunity to testify at this hearing and provide you with our views on data breach legislation and, more particularly, on the Subcommittee's "discussion draft" of the Data Security and Breach Notification Act of 2015.

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

At the outset, NRF would like to thank the members of the Subcommittee and staff for the considerable time and effort they have expended to address this critically important issue to our nation's businesses and consumers. Through this hard work, the Committee on Energy and Commerce is beginning to take steps necessary to help raise the level of data security practices throughout industry and to provide greater consumer awareness and notification of breaches of security when they do occur.

We have spent a great deal of time working with our member companies to present the Subcommittee staff with the retail industry perspective on elements of data security and breach notification since the release of the initial draft bill last summer. We view today's hearing as an opportunity to continue a productive dialogue on how the discussion draft today can be further clarified and improved in substantive respects.

We look forward to working with the Subcommittee members as the bill moves through the upcoming markup and onto the next stages of consideration at the full committee level to help ensure that the legislation ultimately reported by the Committee is as strong and effective as it can be. We also trust that the Subcommittee views the analysis of the discussion draft text we provide in this testimony in the constructive light in which it is intended.

Executive Summary

Maintaining customers' trust is our members' highest priority and, as further detailed in the testimony below, retailers make significant investments in data security with the goal of preventing theft or fraudulent use of customer information. On behalf of our members, NRF has adopted a multi-pronged effort to help improve data security practices, retire fraud-prone payment cards and help in the fight to defend against cyber attacks that threaten all businesses, including retailers. Specifically, these efforts include support for the establishment of a uniform nationwide breach notification standard, promotion of improved payment card security – such as efforts make PIN and chip cards a reality in the United States – and the programs NRF launched 9 months ago to provide our members with a cybersecurity threat information-sharing and a security alert listserv to help disseminate information that could help prevent cyber attacks.

Virtually all of the data breaches we've seen in the United States during the past year – from attacks on the networked systems of retailers, entertainment and technology companies that have been prominent in the news, to a reported series of attacks on our largest banks that have received less attention – have been perpetrated by criminals that are breaking the law. All of these companies are victims of these crimes and we should keep that in mind as we explore this topic and public policy initiatives relating to it.

Additionally, while 51 different U.S. breach notification laws is a nearly nationwide disclosure regime, it is not *uniform*, and it has resulted in a patchwork of notice and other requirements that is neither the most efficient for victimized businesses nor the most effective for consumers. Laws in 47 states and 4 federal jurisdictions (including the District of Columbia) create difficult compliance for our members, particularly mid-sized regional operations that may operate in several states. That is because the applicable state breach notice law is determined by the affected customer's residence, and not the location of the business. The same is true for small and moderately sized online retailers that may have a regional or national footprint. One, uniform nationwide notice standard would help both businesses and consumers by aiding in the provision of effective notice to them when a breach occurs.

Our support for data security breach notification legislation, however, goes beyond support simply for uniformity in application of the law across the United States, as NRF has called for such a law to apply to all businesses that handle sensitive personal information. Establishment of one federal disclosure standard for all businesses handling sensitive customer data will lead to clear, concise and consistent notices to all affected consumers whenever or wherever a breach occurs.

Furthermore, when disclosure standards apply to all businesses that handle sensitive data, it creates the kind of security-maximizing effect that Congress wishes to achieve because all businesses are incentivized to provide greater security in order to avoid public notification of a breach. Exemptions for particular industry sectors would not only ignore the scope of the problem, but create risks criminals can exploit, and disincentives for exempted businesses from making the necessary investment and commitment to improving its data security, because there is no threat of exposure for failures to protect sensitive customer information.

Each of these issues is discussed in greater detail in our written testimony below. To summarize our position on breach notification legislation, NRF has adopted three principles we believe are essential for any proposed federal legislation, as follows:

NRF's 3 Principles for a Federal Breach Notification Law

1. One federal breach notification law that applies to all entities handling sensitive customer data and that establishes the same or similar notice obligations across industry sectors for data breaches;
2. A federal law whose provisions reflect the strong consensus of state laws and, where possible, improve upon deficiencies in those laws that lead to ineffective consumer notice; and
3. A federal law that establishes a uniform, nationwide standard by being truly preemptive of related state laws.

We will offer our more considered views on each of these principles below and, using them as a benchmark, will provide our initial comments on the effectiveness of the discussion draft's provisions to achieve these goals, particularly in the area of notification and preemption. Lastly, we will address the multi-tiered set of data security standards already applying to retailers and ways that retailers are implementing new technologies to help improve the security of their own networks and encourage similar improvements in payment card security used in payment networks not controlled by merchants.

Lastly, before we begin the specific comments on the sections of the bill that relate to our three principles above, we want to first acknowledge and observe that the Subcommittee has addressed previous concerns raised with last summer's draft bill, through textual revisions, so that the current discussion draft features:

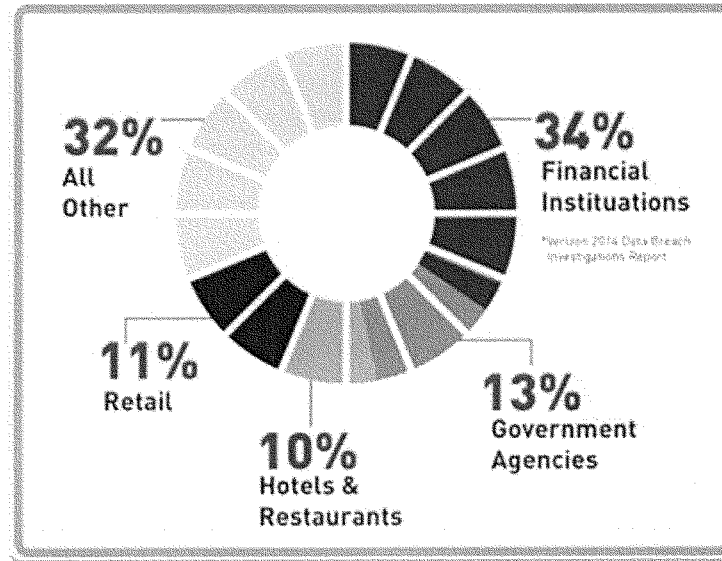
- a more carefully-crafted definition of "covered entity" that includes only entities under the Committee's jurisdiction;
- a definition of "service provider" limited to entities subject to the Communications Act; and
- a revised preemption clause that would not give the benefit of preemption to those who are not subject to bill's obligations.

Legislation Should Require Effective Breach Notice by All Entities Handling Sensitive Data

Unfortunately, data breaches are a fact of life in the United States, and virtually every part of the U.S. economy and government is being attacked in some way. In its 2014 Data Breach Investigations Report, Verizon determined there were 63,347 data security incidents reported by industry, educational institutions, and governmental entities in 2013, and that 1,367

of those had confirmed data losses. Of those, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, and hotels and restaurants combined had 10%. *Figure 1* below illustrates where breaches occur.

Where Breaches Occur (Figure 1)



Source: 2014 Data Breach Investigations Report, Verizon¹

It may be surprising to some, given recent media coverage, that three times more data breaches occur at financial institutions than at retailers. And, it should be noted, even these figures obscure the fact that there are far more merchants that are potential targets of criminals in this area, as there are one thousand times more merchants accepting card payments in the United States than there are financial institutions issuing cards and processing those payments. It is not surprising that the thieves focus far more often on banks, which have our most sensitive financial information – including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.

These figures are sobering; there are far too many data security breaches. These breaches are often difficult to detect and are carried out in many cases by criminals with significant resources behind them. The acute pressure on consumer-serving companies, including those in

¹ 2014 Data Breach Investigations Report by Verizon, available at: <http://www.verizonenterprise.com/DBIR/2014/>

e-commerce, as well as on our financial system, is due to the overriding criminal goal of financial fraud. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality.

The Year of the Breach, as 2014 has been nicknamed, was replete with news stories about data security incidents that raised concerns for all American consumers and for the businesses with which they frequently interact. Criminals focused on U.S. businesses, including merchants, banks, telecom providers, cloud services providers, technology companies, and others. These criminals devoted substantial resources and expertise to breaching the most advanced data protection systems. Vigilance against these threats is necessary, but we need to focus on the underlying causes of breaches as much as we do on the effects of them.

If there is anything that the recently reported data breaches have taught us, it is that any security gaps left unaddressed will quickly be exploited by criminals. We live in a networked world. For example, the failure of the payment cards themselves to be secured by anything more sophisticated than an easily-forged signature makes the card numbers particularly attractive to criminals and the cards themselves vulnerable to fraudulent misuse. Likewise, cloud services companies that do not remove data when a customer requests its deletion, leave sensitive information available in cloud storage for thieves to later break in and steal, all while the customer suspects it has long been deleted. Better security at the source of the problem is needed. The protection of Americans' sensitive information is not an issue on which unreasonably limiting comprehensiveness makes any sense.

In fact, the safety of Americans' data is only as secure as the weakest link in the chain of entities that share that data for a multitude of purposes. For instance, when information moves across communications lines – for transmission or processing – or is stored in a “cloud,” it would be senseless for legislation to exempt these entities, if breached, from comparable data security and notification obligations applying to all other entities that may suffer a breach. Likewise, data breach legislation should not subject businesses handling the same sensitive customer data to different sets of rules with different penalty regimes, as such a regulatory scheme could lead to inconsistent public notice and enforcement.

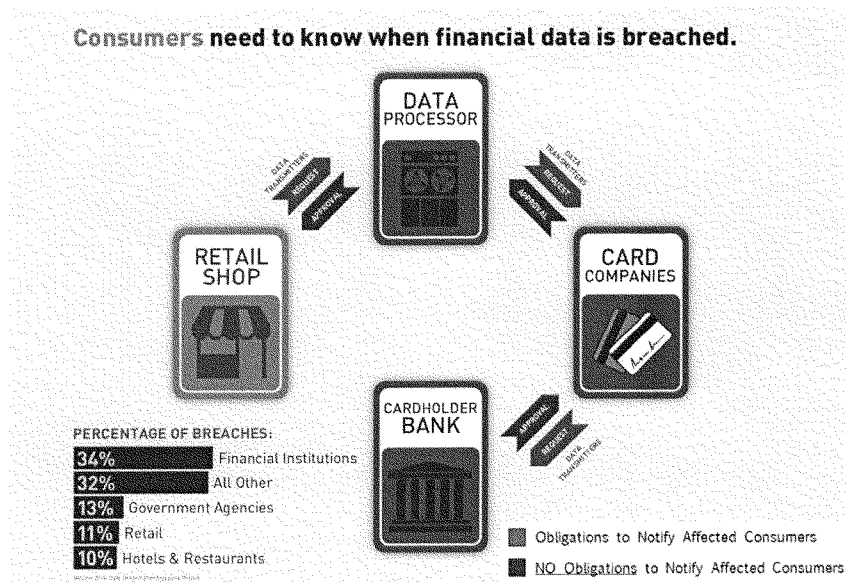
Given the breadth of these invasions, if Americans are to be adequately protected and informed, federal legislation to address these threats must cover all of the types of entities that handle sensitive personal information. Exemptions for particular industry sectors not only ignore the scope of the problem, but create risks criminals can exploit. Equally important, a single federal law applying to all breached entities would ensure clear, concise and consistent notices to all affected consumers regardless of where they live or where the breach occurs.

Third-Party Entities – Insufficient Notice Rule in Section 3(b) of Discussion Draft

Figure 2, below, illustrates how section 3(b)(1) of the discussion draft would operate with respect to notice by “third-party entities” operating in the payment system. This graphic illustrates a typical payment card transaction in which the Energy and Commerce Committee has jurisdiction over all of the entities except for the bank. In a typical card transaction, a payment card is swiped at a card-accepting business, such as a retail shop, and the information is

transmitted via communications carriers to a data processor, which in turn processes the data and transmits it over communications lines to the branded card network, such as Visa or MasterCard, which in turn processes it and transmits it over communications lines to the card-issuing bank. (Typically there also is an acquirer bank adjacent to the processor in the system, which *figure 2* omits to provide greater clarity of the general payment flows.) Section 3(b)(1) of the discussion draft would only require the retail shop, in this example, to provide consumer notice of a breach of security. The data processor, data transmitter or card company suffering a breach would qualify as a third-party whose only obligation, if breached, is to notify the retail shop of their breach – not affected consumers or the public – so that the retailer provides notice on their behalf. And the bank suffering a breach would be exempt from notifying consumers or the public under the discussion draft’s definition of “covered entity” in section 5. Comparing this to *figure 1*, this consumer notice regime presents an inaccurate picture of the breadth of breaches to consumers. Furthermore, such a notice regime is fraught with possible over-notification because payment processors and card companies are in a one-to-many relationship with retailers. If the retailers must bear the public disclosure burden for every other entity in the networked system that suffers a breach, then 100% of the notices would come from the entities that suffer only 11% of the breaches. This is neither fair nor enlightened public policy.

Notice Obligations Should Apply to All Breached Entities (Figure 2)



A recent example illustrates the important point about the risks of over-notifying and confusing American consumers if this proposed third-party notice rule illustrated in *Figure 2* is adopted by the Subcommittee. The largest payment card breach in history occurred at a payment processor, Heartland Payment Systems, which was breached in 2008 and resulted in the compromise of over 130 million payment cards. If Heartland had to follow the proposed third-party notice rule in the discussion draft, rather than notifying the public of its breach as it did, it would have only been obligated to separately notify each of the merchants that it processed payments for, letting them know the affected card numbers that were breached. Those merchants (who were not breached) would, in turn, have had to request (and possibly pay for) the contact information for each cardholder through some arrangement with each affected card company or card-issuing bank, and then make notice to those affected customers and/or make “substitute” notice (where individualized notice cannot be made) by announcing the breach to the general public.

One consequence of this circuitous disclosure process is that it could ultimately lead to over-notification and confusion of consumers about the payment processor’s breach that may affect them. For example, if affected consumers shopped at a number of retailers that all used the same payment processor that suffered the breach (e.g., Heartland, in this hypothetical), the consumers could potentially receive slightly different notices from each store – all providing an account based on what they knew about the breach by the same payment processor – when none of those branded retail stores actually suffered the breach itself. This third-party notice structure would create an untenable public policy “solution” that neither serves consumers nor the multiple non-breached businesses that are providing notice for the breached one.

Just as merchants, such as Target, who have publicly acknowledged a breach have taken tremendous steps to heighten their security, Heartland continued to harden its systems (after notifying of its own breach) and now is recognized as one of the most secure platforms in the industry. The threat of public notice has had a multiplier effect on other commercial businesses.

Indeed, Congress should go further than the proposed third-party entity provision in section 3(b) of the discussion draft: it should establish the *same* data breach notice obligations for *all* entities handling sensitive data that suffer a breach of security. Congress should not permit “notice holes” – the situation where certain entities are exempt from publicly reporting known breaches of their own systems. If we want meaningful incentives to increase security, everyone needs to have skin in the game.

Service Providers – Exemptions from Providing Any Notice under Section 3(e)

Another – and even wider – notice hole that has remained unplugged for many years in other legislative proposals, and remains as a holdover in this discussion draft, is the exemption permitting service providers to avoid notification of their breaches altogether, even when aware of them. Section 3(e) of the discussion draft would permit an entity providing data transmission or storage services to avoid providing consumer or public notice when it is aware of a breach of its data system if it fails to identify them.

Other businesses, such as retailers, however, would be required by the discussion draft to provide notice even if the breached entity does not have the contact information for affected consumers, which is often the case for a retailer when payment cards are breached. In those instances, other covered entities must provide substitute notification. Why not service providers?

The service provider exemption in section 3(e) is drafted so as to permit no notice at all to be made, not even to the FTC or other federal law enforcement for a known breach of security affecting sensitive personal information. Surely Congress should not pass a disclosure law that provides a “free pass” for known breaches of security to certain service providers simply because they have successfully engineered such an exemption in past legislative proposals that had no prospect of passing Congress.

Allowing this type of notice hole in legislation that this Subcommittee would proffer as a “uniform” breach notification bill makes no sense. Just because a telecommunications provider or another company qualifying as a “service provider” may provide a service to another business does not mean it should be permitted to escape providing notice of its data breaches. With an exemption for service providers like the one contained in section 3(e) of the discussion draft, there would be a real risk that the public would not learn of the providers’ breaches in most instances and consumers would not get the information about the breach they need to potentially protect themselves.

Furthermore, under the discussion draft, if a service provider can identify the sender of a transmission that was affected by a breach, it must notify the sender, but then has no further obligations under the bill. This means that, even where it can identify an affected customer, other businesses will have to plug this notice hole and take the attendant cost and blame for providing consumer notice of the service provider’s data breach. The legal liability can be severe, for example, if the service provider does not provide information in a timely fashion such that the non-breached company with the notice obligation cannot make timely notice within 30 days.

The discussion draft’s section 3(e), therefore, amounts to both a *notice-shift* and a *liability-shift* by the breached service provider onto their clients who were not breached but were victimized by using the breached service provider. It begs the question as to what findings the committee has made, and what evidence does it have in the record, to justify this kind of provision, which has no precedent in any of the 47 state breach notification laws. In fact, inclusion of such a provision in a preemptive bill would mean a reduction in disclosure requirements for service providers (as defined in this discussion draft) from the obligations they currently have under state breach notification laws today.

Finally, as noted above, such a notice hole for service providers reduces their incentives to improve their data security systems and protect customer data because it leaves them with no skin in the game even when they suffer a breach of security in their provision of services.

Financial Institution Exemptions – Definition of “Covered Entity” in Section 5

Many legislative proposals last Congress had notice holes, such as those noted above, where consumers would not receive disclosures of breaches by certain entities. Perhaps the notice hole that has been left unplugged in most proposals, and again is left wide open by the discussion draft’s definition of “covered entity” in section 5, is the exemption for financial institutions. We understand and appreciate the *jurisdictional* limitations of the Energy and Commerce Committee at this stage in the process, but it is worth pointing out for the record that the discussion draft’s exempted entities – those subject to the Gramm Leach Bliley Act (GLBA) – do not have any federal statutory language that requires them to provide notice of their security breaches to affected consumers or the public.

Interpretive information security guidelines issued by federal banking regulators in 2005 did not effectively address this lack of a federal notice requirement when it set forth an essentially precatory standard for providing consumer notice in the event that financial institutions were breached. Rather, the 2005 interagency guidelines state that banks and credit unions “should” conduct an investigation to determine whether consumers are at risk due to the breach and, if they determine there is such a risk, they “should” provide consumer notification of the breach.² The existing guidelines for financial institutions fall far short of creating a federal notification “requirement” that the Subcommittee would impose on all other entities by using the language of “shall” – an imperative command used in the discussion draft’s section 3 notification rules (i.e., *see* p. 3, line 1, third word) for entities that would be subject to Federal Trade Commission enforcement. Instead, banks and credit unions are left to make their own determinations about when, and whether, to inform consumers of a data breach.

Several accounts in 2014 of breaches at the largest U.S. banks demonstrate the lack of any notice requirement under the interagency guidelines. It was reported in news media last fall that as many as one dozen financial institutions were targeted as part of the same cyber-attack scheme.³ It is not clear to what extent customers of many of those institutions had their data compromised, nor to our knowledge have the identities of all of the affected institutions been made public. The lack of transparency and dearth of information regarding these incidents reflects the fact that banks are not always subject to the same requirements to notify affected customers of their own breaches of security as other businesses are required now under 47 state laws and would be required under the discussion draft, despite the fact that financial institutions hold Americans’ most sensitive financial information. By comparison, a number of the more seasoned and robust state laws, such as California’s first-in-the-nation breach notification law, have not exempted financial institutions from the state breach notification law because they recognize that banks are not subject to any federal requirement that says they “shall” notify customers in the event of a breach of security affecting them.

² Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS), accessible at: <https://www.fdic.gov/news/news/financial/2005/fil2705.html>.

³ “JP Morgan Hackers Said to Probe 13 Financial Firms,” *Bloomberg* (Oct. 9, 2014).

Conclusion – Proposed General Principle for Effective Notice by All Breached Entities

With respect to establishing a national standard for individual notice in the event of a breach of security at an entity handling sensitive personal information, the only principle that makes sense is that these breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of their own systems.

Just as the Federal Trade Commission (FTC) expects there to be reasonable data security standards employed by each business that handles sensitive personal information, a federal breach notification bill should adopt notification standards that “follow the data” and apply to any entity in a networked system that suffers a breach of security when sensitive data is in its custody.

With respect to those who have called upon the entity that is “closest to the consumer” to provide the notice, we would suggest that the one-to-many relationships that exist in the payment card system and elsewhere will ultimately risk having multiple entities all notify about the same breach – someone else’s breach. This is not the type of transparent disclosure policy that Congress has typically sought. An effort to promote relevant notices should not obscure transparency as to where a breakdown in the system has occurred. Furthermore, for most payment card breaches, the entity closest to the affected customers – the entity that has the affected customers’ contact information because it bills them monthly – is the card-issuing bank that the proposed discussion draft exempts and that the FTC has no jurisdiction over. This is yet another notice hole that applies to the theory of “closest-to-the-consumer” notice in many cases.

This is not to say, however, that a notice provision is impossible to construct that would address the concerns above. In fact, in our discussions with state attorneys general about the deficiencies of the third-party entity notice obligation in their state’s laws, it became apparent that the guiding principle should be “effective” notice, of which relationship to the customer is only one fact, and other considerations such as the speed, uniformity and clarity of the consumer notification must also be taken into account. In the Heartland example above, for instance, the payment processor made substitute notice because that was the most effective way to notify 130 million card holders. It did not follow the deficient third-party entity rule in this discussion draft, and this Subcommittee should not force companies to make ineffective customer notice either.

Indeed, a public notice obligation on all entities handling sensitive data would require consumer notification whenever and wherever a breach occurs. In doing so, it would create significant incentives for every business that operates in our networked economy to invest in reasonable data security to protect the sensitive data in its custody. By contrast, a federal law that permits “notice holes” in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public’s trust.

Legislation Should Establish a Nationwide, Uniform Standard Preemptive of State Law

For more than a decade, the U.S. federalist system has enabled every state to develop its own set of disclosure standards for companies suffering a breach of data security and, to date, 47

states and 4 other federal jurisdictions (e.g., the District of Columbia, Guam, Puerto Rico and the Virgin Islands) have enacted varying data breach notification laws.⁴ Many of the states have somewhat similar elements in their breach disclosure laws, including definitions of covered entities and covered data, notification triggers, timeliness of notification, provisions specifying the manner and method of notification, and enforcement by state attorneys general. But they do not all include the same requirements, as some cover distinctly different types of data sets, some require that particular state officials be notified, and a few have time constraints (although the vast majority of state laws only require notice “without unreasonable delay” or a similar phrase.)

Over the past ten years, businesses such as retailers, which are subject to all of the state and federal territory breach disclosure laws, have met the burden of providing consumer notice, even when they did not initially have sufficient information to notify affected individuals, through the standardized substitute notification procedures in each state law. However, with an increasingly unwieldy and conflicting patchwork of disclosure laws covering more than fifty U.S. jurisdictions, it is time for Congress to acknowledge that the experimentation in legislation that exists at the state level and that defines our federalist system has reached its breaking point, and it is time for Congress to step in to create a national, uniform standard for electronic data in interstate commerce in order to ensure uniformity of a federal act’s standards and consistency of their application across jurisdictions.

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

In order to establish a uniform standard, preemptive federal legislation is necessary. But that does not mean (as some have contended) that the federal standard must or should be “weaker” than the state laws it would replace. On the contrary, in return for preemption, the federal law should reflect a strong consensus of the many state laws. Some stakeholders in breach notice legislation, like NRF, have called for a more robust notification standard at the federal level than currently exists at the state level. Without adding unnecessary bells and whistles, NRF believes that Congress can create a stronger breach notification law by removing the exemptions and closing the types of “notice holes” noted above, thereby establishing a breach notification standard that applies to all businesses – a comprehensive approach the Energy and Commerce Committee and this Subcommittee have adopted in previous consumer

⁴ See, National Conference of State Legislatures (NCSL) website for a complete list of the 51 jurisdictions with breach notice laws, and 3 states without a breach law: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

protection legislation that is now federal law. This approach would enable members that are concerned about preempting state laws to do so with confidence that they have created a more transparent and better notification regime for consumers and businesses alike. It is a way this Committee and Congress can work to enact a law with both robust protection and preemption.

We urge you, therefore, in pursuing enactment of federal breach notification legislation, to adopt a framework that applies to all entities handling sensitive personal information in order to truly establish uniform, nationwide standards that lead to clear, concise and consistent notices to all affected consumers whenever or wherever a breach occurs. When disclosure standards apply to all businesses that handle sensitive data, it will create the kind of security-maximizing effect that Congress wishes to achieve.

Unclear Effect of Preemption Language in Section 6 of Discussion Draft

The discussion draft's section 6 includes a clause intending to preempt the application of state breach laws, but it couples it with a not-yet-finalized, bracketed clause that would preserve a covered entity's "liability under common law." Despite the inclusion of language in the bill's enforcement section that private causes of action cannot be brought against covered entities for "a violation of this Act," inclusion of the preemption clause language preserving common law liability would mean that retailers who are in full compliance with this act's provisions would remain potentially liable under various common law claims by singular or class action plaintiffs.

Furthermore, the federal courts have ruled that a carve-out for some state laws in preemption clauses creates sufficient ambiguity as to Congressional intent as to jeopardize the entire preemption clause (see, e.g., CAN-SPAM Act of 2003). We have urged members' staff in our previous discussions not to construct a preemption clause in a form that may lead to greater uncertainty in the language and, therefore, potential legal challenges to the preemptive effect of the federal law in the 51 jurisdictions where breach laws have been enacted.

Preemption of state laws and common laws that create differing standards of care is never easy, and there is a long history of Supreme Court and other federal courts ruling that, even when Congress expresses an intent to preempt state laws, limiting the scope of the preemption may not result in the preemption of related state laws. In fact, attempts to limit preemption may only result in adding yet another law, this time a federal one, to the panoply of state statutes and common laws already in effect, resulting in the continuation of a confusing tapestry of state law requirements and enforcement regimes. A federal act that leaves this in place would undermine the very purpose and effectiveness of the federal legislation in the first place.

Data Security Standards for General Applicability to Businesses

Collectively, retailers spend billions of dollars safeguarding sensitive customer information and fighting fraud. Maintaining the trust of retail customers by preventing the theft of sensitive personal information related to retail shopping, and the potential fraudulent use of that data by criminals, is at the top of our industry's priorities. It should not be surprising, then, that data security is something in which our members invest heavily and strive to improve every day.

The Subcommittee should keep in mind, though, that security is like defense, and while a retailer could theoretically spend all of its money on defense, it would still not be 100% protected from all attacks. As it is with our national defense and the protection of government facilities alike, the reality of corporate data security is that it is much more difficult to implement than what is theoretically possible, especially if it must be robust enough to defend against attacks like those perpetrated against every sector of American industry from foreign-based criminal organizations that, as we have seen, may be directed, facilitated or tolerated by the host nation states from which they operate and launch their malicious cybersecurity attacks on U.S. corporate networks.

Federal and State Data Security Standards Apply to All Retailers

The Federal Trade Commission (FTC) has often recognized, including in its testimony before Congressional committees, the reality that businesses implementing data security safeguards should not be expected by government to be 100% protective – that is, capable of successfully defending against every attack every time. As a result, the FTC has effectively determined that businesses should be held to “reasonable” data security standards and that the fact of suffering a breach, alone, is not sufficient to determine whether or not a business met this standard. Once again, beyond the theoretical, the reality is that the FTC vigorously enforces a reasonable data security standard against all businesses subject to its jurisdiction.

The FTC has already brought over 50 actions against companies nationwide in a range of industry sectors for what it claims are unreasonable data security practices. The Commission exercises this authority under Section 5 of the FTC Act (15 USC 45), which prohibits “unfair or deceptive acts or practices in or affecting commerce” – a prohibition that applies to all entities engaged in commerce. When the Commission believes a business has fallen short in providing reasonable data security protections for sensitive personal information, it typically (but not exclusively) acts under the “unfairness” prong of Section 5, finding a business in violation where its data security practices cause, or are likely to cause, substantial injury to consumers that cannot be reasonably avoided by those consumers and are not outweighed by countervailing benefits to those consumers or to competition.

This, by definition, is a subjective determination made by the FTC, and not a set of static requirements. Because of this, the FTC’s authority under Section 5 is limited to bringing entities under a cease and desist order for potential violations, and not fining them for data security practices with which they may otherwise not recognize are “unfair” in the eyes of the Commission enforcement attorneys. Nonetheless, rather than face an administratively determined cease and desist order, nearly all of these companies have settled with the FTC, paid fines for their alleged violations (sometimes to the extent of millions of dollars), and agreed to raise their security standards and undergo extensive audits of their practices over the next several decades to ensure that their data security standards are in line with the FTC’s order.

Our members recognize the severity of this federally-imposed data security standard enforced by the FTC under Section 5 of the FTC Act, which applies to all businesses subject to the FTC’s jurisdiction. Additionally retailers are subject to and comply with a range of state

laws specifically governing data security, as well as state consumer protection regulations enforced through their consumer protection agencies and/or their attorneys general. This robust set of existing law, enforced aggressively by the FTC and subject to enforcement by a range of state AGs for data security failures, is a reality, even though some in the financial services community attempt to perpetuate the myth that retailers are not subject to any data security standards under the law.

Payment Card Industry Data Security Standards Apply to All Retailers Accepting Cards

In addition to the federal and state laws, any merchant that accepts bank-issued credit or debit cards from consumers must comply with more than 220 specific data security requirements dictated by the card industry's Payment Card Industry (PCI) Data Security Council. These data security standards, enforced by rules and contract, present another tier of liability and significant annual expense for merchants on top of federal and state government actions. Under the PCI data security standards, card-accepting merchants must protect payment card transactions and submit annually, at considerable cost, to certification processes.

When it comes to protecting payment card data, however, retailers are essentially at the mercy of the dominant credit card companies. The credit card networks – Visa, MasterCard, American Express, Discover and JCB – effectively control the PCI Data Security Council that is responsible for setting the PCI data security standards for payment cards. Unlike other technical standards-setting bodies that are comprised of stakeholders from those industries that have an interest in, and/or will be subject to, the standards, PCI standards are imposed by the payment card industry on all card-accepting businesses across a variety of industries without providing card-accepting businesses any real vote in the standards processes imposed upon them, relegating merchants to near meaningless “advisory” positions, at best. Nevertheless, retailers have spent billions of dollars on card security measures and upgrades to comply with PCI card security requirements, but it hasn't made them immune to data breaches and fraud.⁵

Effect of Imposing GLBA-Like Standards on Businesses Subject to FTC Enforcement

Despite this robust, multi-tiered data security standards and enforcement regime, which includes federal, state and banking industry-imposed data security standards, some in the financial services community attempt to perpetuate the myth that other businesses, including retailers, are not subject to any general data security standards or specific requirements, apparently overlooking the requirements that branded payment networks themselves have already imposed on card-accepting businesses through the PCI Data Security Council that they exclusively control. The members of this Subcommittee should recognize the truth about data security standards borne by card-accepting businesses as it examines this issue, and whether it is necessary and appropriate to impose an additional GLBA-like federal data security standard on top of the existing standards under which these businesses, including retailers, are already complying nationwide.

⁵ The card networks have made those decisions *for* merchants, not *with* merchants, and the increases in fraud demonstrate that *their* decisions have not been as effective as they should have been. In fact, it reflects the reality that specific, operational data security standards are often a generation behind the criminals that invest heavily in developing new methods to defeat what they know to be the industry-prescribed standards.

As a result of the little-understood differences in the data security standards and enforcement regimes faced by banks under the banking regulators versus the standards faced by the wide array of businesses (including retailers) subject to FTC enforcement, not to mention the substantive and well-considered reasons behind those differences in standards and enforcement, we sought an expert opinion on the effect of applying a GLBA-like data security standard to non-financial businesses. Specifically, we asked for an analysis of whether it would be appropriate and effective for proposed federal legislation to impose banking industry based data security standards on the full array of commercial businesses, ranging from large multinational conglomerates to small operations, that are not “financial institutions,” including every non-banking business in America that accepts virtually any form of tender other than cash (e.g., credit cards, debit cards, checks, etc.) from customers in exchange for goods and services.

As part of your efforts to craft data breach legislation, we strongly encourage you to review the white paper attached as *Appendix A* to this testimony, which was just released by two former associate directors responsible for financial and credit practices in the FTC’s Bureau of Consumer Protection. As the excerpts from the white paper below demonstrate, this analysis provides a valuable perspective to the Subcommittee and indicates why we believe the broad expansion of data security standards similar to the GLBA guidelines to virtually every unregulated business in the U.S. economy would be a serious error.

• **Would Cover Virtually All Providers of Consumer Goods and Services:** As noted in the executive summary of the white paper, the authors demonstrate the broad impact from FTC enforcement of GLBA-like data security standards:

“Because of the near-universal acceptance of bank-issued cards as payment for goods and services, companies that would be subject to the Guidelines’ standards would include merchants, hotels, bars and restaurants, theaters, auto dealers, gas stations, grocery and convenience stores, fast-food eateries, airlines and others in the travel industry, hospitals and doctors, dentists, veterinarians, hair salons, gyms, dry cleaners, plumbers and taxi drivers. In other words, virtually all providers of consumer goods and services would be covered.” (emphasis added)

• **Safeguards Designed for Banks are “Poor Fit” for Card-Accepting Businesses:** As the white paper’s analysis explains in greater detail, financial institutions have multi-factored requirements for data security because they routinely have much broader sets of the most sensitive personal and financial customer information in digitized form, which presents security risks and vulnerabilities not evident in most unregulated commercial businesses with much narrower data sets with less sensitive customer information. The authors explain several reasons why data security “safeguards requirements designed for closely supervised banks that issue credit and debit cards are a poor fit for the vast array of entities that accept credit cards and debit cards as payment for their goods and services.” For example:

• **Banking Examination is Interactive Guidance Process; No Comparable Guidance for Vast Array of Businesses under FTC Adversarial Process:** GLBA guidelines are “premised on an ongoing and interactive process between regulator and

regulated entity, whereby examiners can instruct a bank on an apparent failure to meet a specific requirement. This process enables the institution to explain why a particular element of the Guidelines may be inapplicable or to correct any real deficiencies without legal sanctions.” The vast array of businesses subject to FTC jurisdiction have no comparable process. Rather, “the FTC obtains compliance by initiating law enforcement investigations, using compulsory process, when it suspects a potential law violation based on facts that have come to its attention.” The FTC’s “after the fact” adversarial review process may lead to fines imposed on a business for noncompliance of which it may not be aware until it is under investigation by the FTC.

• **Card-Issuers Have Capabilities to Control Card Security; Card-Accepting Businesses Have Least Ability to Ensure Card Security:**

The obligations on card-issuing banks under the GLBA guidelines are “premised on the specific circumstances and capabilities of card **issuers**, which differ substantially from those of entities that accept cards as payment.” It is the banks that dictate to the card-accepting merchants “the card processing capabilities of the equipment and procedures that merchants must use, as well as the security features inherent in the cards.” Furthermore, the authors conclude that: “Were the FTC required to enforce safeguard standards for credit and debit card data based on the Guidelines’ model, it would be imposing obligations on the entities with the least ability to ensure that they were carried out.” In essence, card-accepting businesses do not control the security features of the cards themselves; that is what banks control and one reason why they are subject to GLBA guidelines whereas the FTC made the determination that it is not appropriate to apply the same guidelines to businesses that simply accept payment cards.

• **Would Not Enhance Consumer Protection:** The executive summary concludes by noting that the FTC had previously applying such a rule:

“Subjecting nonbank businesses to the Guidelines’ specific requirements would not enhance the FTC’s ability to use its existing authority to protect consumers through enforcement actions. When it issued consumer information privacy and safeguards rules under the Gramm-Leach-Bliley Act, the FTC considered applying the rules to retailers that accept bank credit or debit cards and declined to do so. We believe that determination remains equally justified today.” (emphasis added)

The different enforcement regimes between financial institutions and entities subject to the FTC’s jurisdiction is also evident in the manner and frequency with which fines are assessed and civil penalties imposed for non-compliance with a purported data security standard. Banks are rarely fined by their regulators for data security weaknesses. But, as noted above, commercial companies paid huge settlement penalties to the FTC. Providing an agency like the FTC, tasked with an adversarial and investigative *enforcement* approach, a set of standards with significant room for interpretation is likely to lead to comparatively punitive actions that are different in kind and effect on entities within the FTC’s jurisdiction than the way the standards would be utilized by banking regulators in an examination. A punitive approach to companies already victimized by a crime would not be appropriate nor constructive in light of the fact that

the FTC itself has testified before Congress that no system – even the most protected one money can buy – is ever 100% secure.

Comments on Data Security Section of Discussion Draft Legislation (Section 2)

In light of the Subcommittee's expedited schedule, we have preliminarily reviewed section 2 of the discussion draft, which provides requirements for information security. The comments below reflect our *initial* views on the draft language of this section:

1. Section 2 Could Expand FTC Enforcement Authority Beyond Existing Reasonable Data Security Standard as the General Rule for All Businesses

While the discussion draft's language is not identical to GLBA data security guidelines, we are concerned that it could be interpreted by the 50 state attorneys general as an expansion of FTC authority in the area of data security enforcement. We understand that other stakeholders may view the following words at the end of the section – “as appropriate for the size and complexity of such covered entity and the nature and scope of its activities” (emphasis added) – as an intended limiting feature to the reasonableness test, but those words could have a different effect in practice. As drafted, these words are in addition to the reasonable standard provided earlier in the section and could create in federal law an additional four-factor test for what constitutes reasonable data security that would go beyond a general standard of “reasonableness” whether cabined in under the unfairness prong or free standing under Section 5 of the FTC Act. This multi-factored test could exponentially increase the risk of a breached company being found at fault by the FTC for a breach, even if the company's data security would have survived an overall reasonableness test under Section 5 of the FTC Act as it is enforced by the FTC today.

For example, this section could be interpreted to mean that the FTC may only have to believe that a company was unreasonable as to any one of the four factors specified in section 2 in order to claim a potential violation of the FTC Act, rather than needing to show that the company had an overall unreasonable data security program. If interpreted in that fashion, it would present an exponentially greater risk because, with four factors, there are 15 ways the FTC could determine a company's program fails this test, and only 1 way a company passes it: that is, if all 4 factors, as applied to its data security program, are independently “reasonable.”

We note that the section 2's information security standard would apply to every type of data that falls within the definition of “personal information” in section 5 of the discussion draft. This means that names, addresses, and birthdates (a combination that is often found in marketing lists and that, alone, generally cannot lead to identify theft) and other typically non-sensitive information must be protected along with more sensitive information such as Social Security Numbers, which could be used to perpetrate fraud and identity theft. This leads to a potentially broader, complex and expensive data security regime for all businesses to implement.

But how does the owner of a chain of dry cleaners, a hair stylist, a veterinarian or a small shopkeeper determine if their data security protection for either payment cards or customer information is reasonable as to the factor of the “size” and “complexity” of its business? Will they understand what that means either directly or in relation to other businesses of their type?

How will they know if they are reasonable as to the “nature” and “scope” of their business activities in the eyes of the FTC? Must these and the vast array of American businesses engage in some kind of comparative analysis between the “size” of other companies or as to the “nature” of their customer information practices – and what does that comparative analysis look like, and what will it cost to obtain? Will every Main Street storefront and service provider in the U.S. now incur costs to hire lawyers in Washington, with specialized FTC practices, simply to ensure that the off-the-shelf equipment and systems for either customer relationship management (CRM) or payment card acceptance will survive an FTC multi-factor reasonableness test? Can they afford not to take this step if the FTC could fine them for non-compliance? And will this require a constant reinvestment in new equipment and/or in new software every single time a more sophisticated attack is discovered that will defeat that technology?

Questions such as the ones above do not come with easy answers, and we do not have them after the limited period of review we have had with this language. However, before the Subcommittee marks up legislation that may add a new information security standard applicable to a vast array of American businesses, we urge it to examine not only the intent of the words it would include in the legislation, but the potential ways such words could be interpreted by the courts, who will turn to the words of the statute itself in applying the law.

Lastly, the FTC’s “reasonable” data security standard enforced today may already take into account the four factors in section 2 above, since those factors are not found in the FTC Act itself. If so, there may be an argument that could be made that there is no need for inclusion of the factors now. Indeed, nearly all state breach laws, including California’s first-in-the-nation breach notification law, that have added a data security standard over the years have used only the word “reasonable” in the statutory text without reference to additional factors. We recommend that the Subcommittee closely examine the data security standards in existing state breach laws and consider the points above before instituting a new, multi-factor test of reasonableness in federal law for broad application to a wide range of commercial businesses.

2. Section 2 Factors Appear to Apply "Guidance Standards" in an FTC Enforcement Regime that is Not Designed to Offer Interactive Guidance to Businesses

Because the FTC is an enforcement agency without the capability, staff or funding to provide supervisory guidance to all businesses under its jurisdiction, even the most sophisticated nationwide businesses that are tasked with designing data security programs in compliance with this new standard would not necessarily know whether and when they would potentially fall out of compliance with the standard before coming under investigation by the FTC.

As noted above in the discussion of the white paper attached as *Appendix A*, unlike the bank examination process where banks engage in an iterative and interactive process with bank examiners to develop a data security program appropriately tailored to the size and complexity of its business and the nature and scope of its information practices in compliance with the GLBA guidance standards, there are no such examiners at the FTC to provide “before-a-breach” guidance on what aspects of a business’s data security program are, or are not, in compliance with the discussion draft’s multi-factor standard that could be enshrined in federal law and enforced with civil penalties imposed by the FTC and state attorneys general.

Since it is unlikely that this Congress would approve a sharp increase in the size of the FTC's staff – perhaps by tens of thousands of examiners – to provide bank-like supervision and guidance to every business in America, this Subcommittee, which has oversight responsibility for the FTC, should consider the potential impact of imposing guidance-like language, similar to GLBA, on every non-financial business in America under an FTC enforcement regime run by an agency that is incapable of providing the basic guidance and interactive process necessary to ensure businesses have an opportunity to be in compliance with these standards.

3. Section 4 Would Grant the FTC Authority to Fine Any Businesses it Deems in Non-Compliance Before the Business Could Even Know It Is Out of Compliance

As noted above, companies have no opportunity to obtain supervisory guidance from the FTC to ensure they are in compliance with what the FTC (in its own discretion) determines is "reasonable" information security under the four-factor test of section 2. Nevertheless, even without the chance of knowing that they may be out of compliance until they come under an FTC investigation, these companies would still face the prospect that the FTC can immediately impose civil penalties on them for claimed violations of section 2 because this provision would be enforced under the trade regulation rules in section 4 of the discussion draft (e.g., "a regulation under Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))").

Unlike the FTC's existing authority under the FTC Act's Section 5 today, the bill would not require the FTC to first bring a company under a cease-and-desist order for noncompliance before it could go straight to imposing fines on it for violations of the Act. This type of civil penalty authority under the trade regulation rules is more justified for enforcement of clear disclosure requirements where the threat of government fines serves as a deterrent to bad actors shunning the law (i.e., the reason why it was authorized in the CAN-SPAM Act of 2003).

Unlike regulated banks who work with examiners to get a data security program right, companies subject to FTC enforcement under section 4 would have no way to determine if they are passing the section 2 test for reasonable data security before being subject to potentially millions of dollars in government-imposed fines. We recommend the Subcommittee reconsider the application of trade regulation rule enforcement to section 2's subjective data security standard, and consider maintaining the same enforcement authority the FTC has today under Section 5 of the FTC Act for unfair or deceptive acts or practices.

4. Consequences of Potential Expansion of FTC Enforcement Authority

Pulling together the potential consequences of the discussion draft's section 2 information security standard and section 4's enforcement standard that are raised in the more detailed comments above, the proposed provision would appear to an expansion of the FTC's existing enforcement authority and a potential extension of the reasonable data security standard it currently enforces into a GLBA-like multi-factor guidance test to apply to all non-financial

companies.⁶ It is important to note that, as coupled with section 4's enforcement language, this standard would be enforced against these companies in a much more severe way than GLBA is enforced against financial institutions. What is being proposed in the discussion draft may therefore be considered to be beyond any rule the banks have in terms of enforcement for programs designed to protect and secure the most sensitive personal and financial information.

Congress should be cautious in weighing in on the question of FTC authority when the agency has pending litigation on the extent of that authority. This is especially important given a government enforcement agency's natural inclination to rush in to determine "who killed the cat" whenever there is a "dead cat" on the floor (i.e., in this instance, when a data breach has occurred). Following breaches, the victim of a crime that had in place reasonable data security practices prior to the breach may, nonetheless, be accused of malfeasance when the organized criminal organization that perpetrated the crime cannot be identified or prosecuted.

Congress should recognize that these criminals have developed and used technology to breach networked systems that is often superior to the state-of-the-art data security technology available to U.S. companies from security vendors. As a result, the Subcommittee ought to be wary of attempts to codify new, statutorily-based and subjectively-determined data security rules (that would be enshrined in the federal law separate and apart from the "unfairness prong" of Section 5 of the FTC Act) to apply to all business in America where: (i) these businesses are not engaged in financial services, as previously determined by the FTC; (ii) the FTC cannot provide bank-like supervisory guidance as to how a business's specific program may come into compliance with the law; and (iii) the subjective standard would be enforced with government fines (not just cease-and-desist orders) against businesses who cannot know in advance if they are in compliance or not.

Conclusion Regarding Generally Applicable Data Security Standards in Legislation

As noted above, NRF and its members support data security standards, and if a standard is to be included in federal breach legislation, it needs to be a general standard that is appropriate to the broad array of businesses it would cover (similar to FTC Act Section 5's prohibitions on "unfair or deceptive acts or practices") and, because it is general, must be enforced consistent with the Commission's long-standing practices under Section 5.

⁶ For those who point out that it is not GLBA, we agree that the proposed discussion draft section 2 provision is not identical to the data security guidelines that apply to financial institutions, but nor should it be, given the significant differences between the most sensitive customer information and complex financial data sets held by financial institutions, a combination with unique vulnerabilities and risks that do not apply to most every other business in America. But section 2, especially when subject to FTC enforcement and civil penalty authority, is also not a lower standard or "GLB-lite," as some have suggested, because banks would not be subject to the imposition of fines for a first violation of subjective standards section 2 would impose. Section 2 would, in fact, apply a stricter enforcement regime on every business in the U.S. for the protection and security of information that is typically much less sensitive than the information banks themselves hold. As Congress should recognize, the imposition of higher standards and more severe penalties for the protection of less sensitive information is not one of the "Fair Information Practice Principles."

Proper Scope of Breach Law – Definition of “Personal Information” in Discussion Draft

In general, the draft bill requires “personal information” (or “PI”) to be protected and secured against “unauthorized access,” and if any PI is accessed or acquired in a breach of security, public notification may be required depending on the type of entity suffering the data breach (as noted above). Notably, the bill contains an expanded definition of PI that is much broader than the PI definitions in most state laws. For example, the combination of a customer’s name, address and birthdate is now considered to be PI. Similarly, a “unique account identifier,” such as one used for CRM purposes, is also considered PI.

This expansive definition of PI could, if enacted as drafted, impact a business’s operation while not providing any corresponding benefit to consumers either from breach notification or increased security of certain types of PI included in the discussion draft’s definition. Additionally, the inclusion of some types of information in the definition of PI may have the unintended consequence of discouraging security steps that businesses might otherwise take to minimize sensitive data in their systems through use of non-sensitive “unique account identifiers.” Several examples of problematic data elements in the PI definition are as follows:

- Name+Address+Birthdate or Name+Phone+Birthdate:** The definition’s inclusion of a combination of a name, address/phone and birthdate is overly broad and portends to sweep in a significant amount of marketing or CRM data that, if breached, would not (alone) lead to identity theft. This combination of information, for example, might be used by retailers and restaurants for promotional reasons (e.g., providing a discounted gift or dinner on your birthday) or to narrow offerings to certain eligible groups (e.g., catalog or promotion for seniors). In fact, it is hard to determine the intended purpose of breach notification for this combination of information – without other information also being breached – if no harm is reasonably likely to result from it and if there is nothing further a consumer might do to protect himself or herself once notified that a marketing list with this information was lost. These may be some of the reasons why most state breach notice laws do not include this combination in their definitions of covered data for breach notification purposes. Additionally, because the bill requires all PI to be protected with information security, inclusion of this combination of non-sensitive “phone book” or market segmentation information will need to be as protected as the most sensitive information, such as Social Security Numbers maintained by a business in its HR/employee records. The increased cost to secure benign marketing data may be absorbed by reductions in the amount of promotions offered to consumers even though there is no concomitant benefit to consumers from the additional security required under the bill. Lastly, we note that the definition of PI excludes information that is derived from public sources, and yet the combinations of “phone book” data in this section could exclusively come from public sources in most cases, raising additional questions as to the necessity of these combinations in the definition of PI.
- Unique Account Identifiers:** The PI definition would also include a “unique account identifier...in combination with any associated security code [etc.]...that is required for an individual to obtain money, or purchase goods, services, or any other

thing of value.” This is an extraordinarily broad element of PI that could possibly include a shopper’s phone number (a unique account identifier) entered into a numeric pad on a store’s point-of-sale system to obtain a discount (based on a loyalty program) in connection with a store purchase. We are not aware of any state breach law that would include as PI a stand-alone phone number, and yet in this scenario, one might be covered by this discussion draft’s definition and require notification if breached. Additionally, as retailers strive to minimize data by replacing sensitive data with tokens (unique account identifiers), inclusion of what has traditionally been seen as non-PI unique identifiers in the definition may discourage companies from making the investment to de-identify or minimize sensitive data if it will still be subject to the same data security standards and lead to notification following a breach, even if that unique account identifier could not directly be used (alone, and without more associated sensitive information tied to it that is also breached with it) to identify or harm an individual. If the discussion draft is to continue to have unique account identifiers in the definition, then to address the concerns above, we would recommend it be qualified, at a minimum, by requiring that such identifiers are only PI if they could “alone be used to gain access to an individual’s account” for the purposes of obtaining money or purchasing goods or services.

Improving Technology Solutions to Better Protect Consumers in Payment Transactions

Improving Payment Card Security

On October 17, 2014, the President signed an executive order initiating the BuySecure Initiative for government payment cards.⁷ The order provided, among other things, that payment cards issued to government employees would include PIN and chip technology and that government equipment to handle and process transactions would be upgraded to allow acceptance of PIN and chip. These are common-sense actions that recognize that, while it may not be possible to ensure there is never another data security breach, it is still possible to minimize the harms that can come from those breaches – and reduce the incentives from criminals to try to steal some data in the first place.

An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. Requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This ought to happen not only in the brick-and-mortar environment in which a physical card is used but also in the online environment in which the physical card does not have to be used. Many U.S. companies, for example, are exploring the use of a PIN for online purchases. This may help directly with the 90 percent of U.S. fraud which occurs online. It is not happenstance that automated teller machines (ATMs) require the entry of a PIN before dispensing cash. Using the same payment cards for purchases should be just as secure as using them at ATMs.

⁷ Executive Order – Improving the Security of Consumer Financial Transactions, The White House, October 17, 2014. Accessible at: <http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>

End-to-End Encryption

Another technological solution that could help deter and prevent data breaches and fraud is encryption. Merchants are already required by PCI standards to encrypt cardholder data but, not everyone in the payments chain is required to be able to accept data in encrypted form. That means that data may need to be de-encrypted at some points in the process. Experts have called for a change to require “end-to-end” (or point-to-point) encryption which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the data in encrypted form.

According to the September 2009 issue of the Nilson Report “most recent cyberattacks have involved intercepting data in transit from the point of sale to the merchant or acquirer’s host, or from that host to the payments network.” The reason this often occurs is that “data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can’t accept encrypted data at this time.”⁸

Keeping sensitive data encrypted throughout the payments chain would go a long way to convincing fraudsters that the data is not worth stealing in the first place – at least, not unless they were prepared to go through the arduous task of trying to de-encrypt the data which would be necessary in order to make use of it. Likewise, using PIN-authentication of cardholders now would offer some additional protection against fraud should this decrypted payment data be intercepted by a criminal during its transmission “in the clear.”

Tokenization and Mobile Payments

Tokenization is another variant that could be helpful. Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the “token”). Sensitive payment data could be replaced with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.⁹ Still, tokenization is not a panacea, and it is important that whichever form is adopted be an open standard so that a small number of networks not obtain a competitive advantage, by design, over other payment platforms

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers won’t need to have a physical card – and they certainly won’t replicate the security problem of physical cards by embossing their account numbers on the outside of their mobile phones. It should be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords. Indeed, if we are looking to leapfrog the already aging current technologies, mobile-driven payments may be the answer.

⁸ The Nilson Report, Issue 934, Sept. 2009 at 7.

⁹ For information on Shift4’s 2005 launch of tokenization in the payment card space see <http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lcts-merchants-re-use-credit>.

Indeed, as much improved as they are, the proposed chips to be slowly rolled out on U.S. payment cards are essentially dumb computers. Their dynamism makes them significantly more advanced than magstrips, but their sophistication pales in comparison with the common smartphone. Smartphones contain computing powers that could easily enable comparatively state-of-the-art fraud protection technologies. In fact, “the new iPhones sold over the weekend of their release in September 2014 contained 25 times more computing power than the whole world had at its disposal in 1995.”¹⁰ Smart phones soon may be nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

The dominant card networks have not made all of the technological improvements suggested above to make the cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe.

In this section, we have merely described some of the solutions available, but the United States isn’t using any of them the way that it should be. While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft, the card networks have arranged the establishment of the data security requirements and yet, in light of the threats, there is much left to be desired.

Legislative Solutions Beyond Breach Notification

In addition to federal legislation, in line with our principles, that would standardize and streamline the breach notification process so that consumers may be treated equally across the nation when it comes to the disclosure of data security breaches affecting them, NRF also supports a range of legislative solutions that we believe would help improve the protection of debit card holders, the security of our networked systems, and the law enforcement tools that could be employed to address criminal intrusions.

Legislation Protecting Consumers’ Debit Cards to the Same Extent as Credit Cards

From the perspective of many consumers, one type of payment cards has often been as good as another. Consumers, however, would be surprised to learn that their legal rights, when using a debit card – i.e., their own money – are significantly less than when using other forms of payment, such as a credit card. It would be appropriate if policy makers took steps to ensure that consumers’ reasonable expectations were fulfilled, and they received at least the same level of legal protection when using their debit cards as they do when paying with credit.

NRF strongly supports legislation like S. 2200, the “Consumer Debit Card Protection Act,” cosponsored by Senators Warner and Kirk last Congress. S. 2200 was a bipartisan solution that would immediately provide liability protection for consumers from debit card fraud to the same extent that they are currently protected from credit card fraud. This is a long overdue correction in the law and one important and productive step Congress could take immediately to protect consumers that use debit cards for payment transactions.

¹⁰ “The Future of Work: There’s an app for that,” *The Economist* (Jan. 3, 2015).

Legislation Protecting Businesses that Voluntarily Share Cyber-Threat Information

NRF also supports the passage by Congress of cybersecurity information-sharing legislation like H.R. 624, the “Cyber Intelligence Sharing and Protection Act,” cosponsored last Congress by Congressmen Rogers and Ruppersberger, which passed the House with bipartisan support. Legislation like this would protect and create incentives for private entities in the commercial sector to lawfully share information about cyber-threats with other private entities, and with the federal government, in real-time. This could help companies better defend their own networks from cyber-attacks detected elsewhere by other business.

Legislation Aiding Law Enforcement Investigation and Prosecution of Breaches

We also support legislation that would provide more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers’ information are swiftly brought to justice.

Conclusion

In summary, a federal breach notification law should contain three essential elements:

1. **Require Public Notice for All Businesses Handling Sensitive Data:** Breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of their own systems. A federal law that permits “notice holes” in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public’s trust.
2. **Reflect the Strong Consensus of State Laws:** A national standard should reflect the strong consensus of state law provisions. NRF believes that Congress can create a stronger breach notification law by removing the exemptions and closing the types of “notice holes” that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses, similar to the comprehensive approach this Committee has taken in previous consumer protection legislation that is now federal law.
3. **Establish Uniform Nationwide Standard through Express Preemption of State Law:** A single, uniform national standard for notification of consumers affected by a breach of sensitive data would provide simplicity, clarity and certainty to both businesses and consumers alike. Passing a federal breach notification law is a common-sense step that Congress should take now to ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.

Appendix A:

White Paper on Data Security Standards

(See separate attachment)

The Effect of Applying Customer Information Safeguard Requirements for Banks
to Nonfinancial Institutions

Joel Winston and Anne Fortney
March 2015

We have been asked to analyze the effect of legislation requiring the Federal Trade Commission (“FTC”) to apply standards based upon the Interagency Guidelines for banks in Safeguarding Customer Information (“Interagency Guidelines” or “Guidelines”) to any entity that accepts bank-issued payment cards for goods and services and does not extend credit itself.

Summary

The Interagency Guidelines for Safeguarding Customer Information apply to depository institutions (“banks”) subject to supervisory examination and oversight by their respective regulatory agencies. The Guidelines contain detailed elements of an information safeguards program tailored specifically to banks. They are designed to be a point of reference in an interactive process between the banks and their examiners, with emphasis on compliance on an on-going basis. The FTC has issued a Safeguards Rule applicable to the nonbank “financial institutions” under its jurisdiction. The Safeguards Rule provides for more flexibility and less specificity in its provisions than do the Guidelines. The more general requirements of the FTC’s Rule are designed to be adaptable to ever-changing security threats and to technologies designed to meet those threats.

The differences in the approaches to data security regulation between the Guidelines and the FTC Safeguards Rule reflect two fundamental differences between the bank regulatory agencies (the “Agencies”) and the FTC: the substantial differences in the types and sizes of entities within the jurisdiction of the Agencies versus the FTC, and the equally substantial differences in the roles played by the Agencies and the FTC in governing the behavior of those entities. With respect to the former, while the banks covered by the Guidelines are relatively homogeneous, extending the Guidelines to all entities that accept payment cards would sweep in a vast array of businesses ranging from large multinational conglomerates to small operations, and could also include individuals.¹ The threats faced by these widely diverse businesses are likely to vary widely as well, as would the sophistication and capabilities of the entities themselves for addressing the threats. A flexible approach as in the Safeguards Rule is necessary to account for those critical differences. Many of the Guidelines’ provisions, which were drafted with banks in mind, likely would be unsuitable for a significant proportion of the entities that would be subject to these new requirements.

¹ Because of the near-universal acceptance of bank-issued cards as payment for goods and services, companies that would be subject to the Guidelines’ standards would include merchants, hotels, bars and restaurants, theaters, auto dealers, gas stations, grocery and convenience stores, fast-food eateries, airlines and others in the travel industry, hospitals and doctors, dentists, veterinarians, hair salons, gyms, dry cleaners, plumbers and taxi drivers. In other words, virtually all providers of consumer goods and services would be covered.

For similar reasons, the different approaches the Agencies and the FTC take in regulating their entities make it problematic to apply the Guidelines to the nonbank entities overseen by the FTC. The more specific Guidelines make sense when, as is the case with the banks, there is an ongoing, interactive dialogue between the regulated entities and the regulator through the supervision process. The regulated entities and regulators can address changes in threats and technologies during the less formal examination process and head-off potential problems before they happen. By contrast, the Safeguards Rule's flexible requirements are better suited to a law enforcement agency like the FTC that obtains compliance not by an interactive dialogue, but by prosecuting violations after-the-fact. Indeed, an entity within the FTC's jurisdiction may have no indication of deficiencies in its compliance until it is under investigation. With the untold numbers of entities potentially subject to its jurisdiction, the FTC simply lacks the capability or resources to engage in dialogue or provide the individualized, ongoing guidance like the Agencies do with their banks.

While the Guidelines would be made applicable to any entity that accepts bank-issued payment cards,² the Guidelines' specific requirements are suitable only for the bank card-issuers that dictate the card processing equipment and procedures for businesses that accept their cards, as well as the security features inherent in the cards. If the Guidelines were made applicable to businesses that merely accept banks' cards, they would impose security obligations on those with the least ability to implement the requirements applicable to payment card security.

Finally, nonbank businesses are subject to the FTC's general authority under the FTC Act to prohibit unfair or deceptive practices, and the FTC has prosecuted many companies under this authority for failing to protect consumer's nonpublic information. Subjecting nonbank businesses to the Guidelines' specific requirements would not enhance the FTC's ability to use its existing authority to protect consumers through enforcement actions. When it issued consumer information privacy and safeguards rules under the Gramm-Leach-Bliley Act, the FTC considered applying the rules to retailers that accept bank credit or debit cards and declined to do so. We believe that determination remains equally justified today.

Our Qualifications

Joel Winston served for 35 years in the FTC's Bureau of Consumer Protection. For nine years, he headed the FTC's offices responsible for consumer information privacy and security, serving as Associate Director for Financial Practices (2000-2005) and for Privacy and Identity Protection (2005-2009). His responsibilities included the development of the FTC Safeguards Rule in 2000-2001, and he directed the FTC's enforcement of that Rule and other consumer protection laws.

² Bank-issued payment cards include credit cards, debit cards and prepaid cards.

Anne Fortney has 39 years' experience in the consumer financial services field, including directing FTC enforcement and rulemaking under the federal consumer financial protection laws as the Associate Director for Credit Practices of the Bureau of Consumer Protection.

We both regularly counsel consumer financial services clients on their compliance obligations. We also assist clients in Consumer Financial Protection Bureau ("CFPB") examinations and in the defense of FTC and CFPB investigations and enforcement actions. In addition, we have each testified multiple times as invited witnesses before U.S. Congressional Committees and Subcommittees on various consumer financial protection laws. We each serve from time to time as subject matter experts in litigation in the federal courts involving consumer financial services.

Background

Federal Requirements for Safeguarding Customer Information

Section 501(b) of the Gramm-Leach Bliley Act ("GLBA" or the "Act")³ required each of the federal bank regulatory agencies (the "Agencies")⁴ and the FTC to establish standards for the financial institutions subject to their respective jurisdictions with respect to safeguarding consumers' nonpublic, personal financial information. The Act required that the safeguards ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.⁵

Interagency Guidelines

Because they exercise supervisory responsibilities over banks through periodic examinations, the Agencies issued their GLBA customer information safeguard standards in the form of Guideline document ("Interagency Guidelines" or "Guidelines").⁶

The Guidelines instruct banks on specific factors that serve as the basis for the Agencies' review during supervisory examinations. They are predicated on banks' direct control over the security of their customers' nonpublic personal financial information.

³ Gramm-Leach-Bliley Financial Modernization Act, Pub. L. 106-102, § 501(b) (1999), codified at 15 U.S.C.A. § 6801(b).

⁴ These were the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS"). In October 2011, as a result of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the OTS was terminated and its functions merged into the OCC, FRB, and FDIC.

⁵ 15 U.S.C.A. § 6801(b).

⁶ Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616-01 (Feb. 1, 2001) and 69 Fed. Reg. 77610-01 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (FRB); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). The Agencies later issued an interpretive Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736-01 (Mar. 29, 2005). This paper includes this interpretive Interagency Guidelines in the summary of the Interagency Guidelines.

They instruct each bank to implement a comprehensive written information security program, appropriate to its size and complexity, that: (1) insures the security and confidentiality of consumer information; (2) protects against any anticipated threats or hazards to the security or integrity of such information; and (3) protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Guidelines provide specific instructions for banks in the development and implementation of an information security program. A bank must:

- Involve the Board of Directors, which must approve the information security program and oversee the development, implementation and maintenance of the program;
- Assess risk, including reasonably foreseeable internal and external threats, the likelihood and potential damage of these threats, and the sufficiency of the bank's policies and procedures in place to control risk;
- Design the program to control identified risks. Each bank must consider whether the following security measures are appropriate for the bank, and, if so, adopt the measures it concludes are appropriate:
 - Access controls on customer information systems;
 - Access restrictions at physical locations containing customer information;
 - Encryption of electronic customer information;
 - Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
 - Dual control procedures;
 - Segregation of duties, and employee background checks for employees responsible for customer information;
 - Response programs that specify actions to be taken when the bank suspects or detects unauthorized access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
 - Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards;
- Train staff to implement the information security program;
- Regularly test key controls, systems, and procedures of the information security program;
- Develop, implement, and maintain appropriate measures to properly dispose of customer information and consumer information;
- Adequately oversee service provider arrangements, including by contractually requiring service providers to implement appropriate procedures and monitoring service providers;
- Adjust the program in light of relevant changes in technology, sensitivity of consumer information, internal and external threats, the bank's own changing business arrangements, and changes to customer information systems;
- Report to the Board of Directors at least annually; and

- Provide for responses to data breaches involving sensitive customer information,⁷ which should include –
 - Developing a response program as a key part of its information security program, which includes, at a minimum, procedures for assessing the nature and scope of an incident;
 - Notifying the bank's primary federal regulator as soon as the bank becomes aware of the breach;
 - Notifying appropriate law enforcement authorities;
 - Containing and controlling the incident to prevent further unauthorized access to or use of consumer information; and
 - Notifying consumers of a breach when the bank becomes aware of an incident of unauthorized access to sensitive customer information. The notice must include certain content and must be given in a clear and conspicuous manner and delivered in any manner designed to ensure the customer can reasonably be expected to receive it.

FTC Safeguards Rule⁸

The FTC protects consumers against “unfair and deceptive acts and practices in or affecting commerce.”⁹ Its jurisdiction includes “all persons, partnerships, or corporations,” except banks, savings and loan institutions, federal credit unions and certain nonfinancial entities regulated by other federal agencies.¹⁰ The FTC issues substantive rules, such as the Safeguards Rule, when required by Congress to do so,¹¹ but it is not authorized to conduct supervisory examinations of entities under its broad jurisdiction. Rather, the FTC is primarily a law enforcement agency.

Because the FTC lacks supervisory examination authority, it issued a Safeguards Rule, rather than Guidelines, to establish customer information safeguards for “financial institutions” under its jurisdiction. The GLBA’s broad definition of “financial institution” includes a myriad of nonbank companies that operate in the consumer financial services industry.¹² The definition includes finance companies, auto dealers, debt collectors and consumer reporting agencies,

⁷ Sensitive customer information includes: a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account, and any combination of components of customer information that would allow someone to log onto or access the customer's account (i.e., user name and password, or password and account number). 12 C.F.R. Part 30, app. B, supp. A, § III.A.1; 12 C.F.R. Part 208, app. D-2, supp. A, § III.A.1, and Part 225, app. F, supp. A, § III.A.1; 12 C.F.R. Part 364, app. B, supp. A, § III.A.1; and 12 C.F.R. Part 570, app. B, supp. A, § III.A.1.

⁸ FTC Safeguards Rule, 16 CFR Part 314. The FTC issued the final rule in 2001.

⁹ 15 U.S.C.A. § 45(a)(1). The FTC Act also prohibits unfair methods of competition in or affecting commerce.

¹⁰ 15 U.S.C.A. § 45(a)(2). For example, the FTC Act exempts not-for-profit entities and common carriers subject to the Communications Act of 1934.

¹¹ The FTC has more general rulemaking authority under Section 18 of the FTC Act, 15 U.S.C.A. § 57a, but has promulgated very few rules under that section in recent years.

¹² See 15 U.S.C.A. § 6809(3) (defining “financial institution” to include any institution engaging in “financial activities”); 12 U.S.C.A. § 1843(k) (defining “financial activities” broadly to include activities that are “financial in nature or incidental to such financial activity” or “complementary to a financial activity”).

among many others. The FTC determined that the final Rule would not apply to retailers that merely accept payment cards, but rather, only to those that extend credit themselves, and only then to the extent of their credit granting activities.¹³

In recognition of the great variety of businesses covered by the Safeguards Rule, the FTC developed a rule that provided for flexible safeguard procedures that could be adapted to the myriad ways in which covered entities are structured and operate. The FTC Rule requires a financial institution to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the entity's size and complexity, the nature and scope of its activities, the types of risks it faces, and the sensitivity of the customer information it collects and maintains. The information security program must: (1) ensure the security and confidentiality of consumer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

In its development, implementation, and maintenance of the information security program, the financial institution must:

- Designate an employee or employees to coordinate the program;
- Identify reasonably foreseeable internal and external risks to data security and assess the sufficiency of safeguards in place to control those risks in each relevant area of the financial institution's operations (i.e., employee training, information systems, prevention/response measures for attacks);
- For all relevant areas of the institution's operations, design and implement information safeguards to control the risks identified in the risk assessment, and regularly test and monitor the effectiveness of key controls, systems, and procedures;
- Oversee service providers, including by requiring service providers to implement and maintain safeguards for customer information; and
- Evaluate and adjust the program in light of material changes to the institution's business that may affect its safeguards.

¹³ See 16 C.F.R. §§ 314.2(a) (adopting the Privacy Rule's definition of "financial institution"). That definition includes examples of "financial institutions," among them: retailers that extend credit by issuing their own credit cards directly to consumers; businesses that print and sell checks for consumers; businesses that regularly wire money to and from consumers; check cashing businesses; accountants; real estate settlement service providers; mortgage brokers; and investment advisors. 16 C.F.R. § 313.3(k)(2). The FTC also opined that debt collectors are "financial institutions." 65 Fed Reg. 33646; 33655 (May 24, 2000). Further, the Privacy Rule also gives examples of entities that are *not* "financial institutions": retailers that only extend credit via occasional "lay away" and deferred payment plans or accept payment by means of credit cards issued by others; retailers that accept payment in the form of cash, checks, or credit cards that the retailer did not issue; merchants that allow customers to "run a tab"; and grocery stores that allow customers to cash a check or write a check for a higher amount than the grocery purchase and obtain cash in return. *Id.* at (k)(3).

When it promulgated this rule, the FTC considered requiring more specific and detailed data security requirements, but determined that doing so would have imposed significant regulatory burdens in light of the broad range of entities potentially subject to the Safeguards Rule.

Comparison of the Interagency Guidelines and the FTC Rule

Both the Interagency Guidelines and the FTC Rule apply only to “financial institutions” with respect to the “nonpublic personal” financial information they collect and maintain. Unlike the Guidelines, however, the FTC Rule applies to many types of entities whose principal business may not involve the provision of financial services to consumers.

While the Guidelines and the FTC Rule share some common elements, they differ in critical respects. In particular, the Interagency Guidelines, which are tailored to closely supervised and regulated banks, are much more detailed in their requirements. These requirements are designed to be the point of reference in an interactive process between the banks and their examiners. As their name implies, the Guidelines are intended to guide banks’ compliance on a going forward basis.

In contrast, the FTC Rule is significantly less specific in its data security requirements than the Guidelines, because the Rule applies to a much broader and more diverse group of entities with wider variations in the data they collect and maintain, the risks they face, and the tools they have available to address those risks. The more general requirements of the FTC Rule also are designed to be adaptable to the near-constant changes in threats, security technologies, and other evolutionary developments in this extremely dynamic area. Whereas the Agencies can address new developments through the interactive examination process, the FTC only has the blunt instrument of law enforcement. And, whereas the Agencies actively supervise and monitor the activities of the entities they oversee, the FTC can only investigate and, if appropriate, take enforcement action against a fraction of the entities over which it has jurisdiction. The FTC’s primary focus is on prosecuting past or existing deficiencies, and a company may receive no advance warning of a possible violation of the Safeguards Rule until it is confronted with an adversarial investigation. The Agencies’ goal, on the other hand, is to prevent future deficiencies by working with the bank on an ongoing basis.

Effect of an FTC Standard That Would Apply Interagency Guidelines to Nonbanks That Do Not Extend Credit and Only Accept Credit Cards

For several reasons, safeguards requirements designed for closely supervised banks that issue credit and debit cards are a poor fit for the vast array of entities that accept credit cards and debit cards as payment for their goods and services. First, as explained above, the Guidelines are premised on an ongoing and interactive process between regulator and regulated entity, whereby examiners can instruct a bank on an apparent failure to meet a specific requirement. This process enables the institution to explain why a particular element of the Guidelines may be inapplicable or to correct any real deficiencies without legal sanctions.

No such process is possible for entities subject to FTC oversight. The FTC obtains compliance by initiating law enforcement investigations, using compulsory process, when it suspects a potential law violation based on facts that have come to its attention. This “after the fact” review focuses, through an adversarial process, on the legal requirements or prohibitions that may have been violated. If violations are found, the FTC seeks a formal order prohibiting the illegal conduct and, in appropriate cases, imposing fines or redress to injured consumers. The FTC lacks supervisory examination authority and lacks the resources to provide the specific guidance and ongoing oversight that would be necessary to effectuate Guidelines-type rules covering the huge diversity of nonbank entities. The result would be comparable to the widespread confusion and noncompliance that resulted from the FTC’s attempt to so broadly define “creditors” subject to its Red Flags Rule¹⁴ that the Rule would apply to types of businesses (such as plumbers, dry cleaners, hospitals, and restaurants) for which the Rule requirements made little sense. Congress had to correct that result with legislation that “reined in” the FTC by limiting the rule to the kinds of “creditors” that need written procedures to detect and prevent identity theft, rather than virtually every consumer-facing business.¹⁵

Second, many of the specific requirements of the Guidelines simply are not relevant to, or would impose unreasonable obligations on, nonbanks. For example, with respect to credit and debit cards, the Guidelines’ obligations are premised on the specific circumstances and capabilities of card *issuers*, which differ substantially from those of entities that accept cards as payment. It is the card issuers, and not the card-accepting merchants, be they hotels or veterinarians, that dictate the card processing capabilities of the equipment and procedures that merchants must use, as well as the security features inherent in the cards. Although chip and PIN technology could reduce card fraud, and many retailers have demonstrated a willingness to install terminals to accept cards with that technology, only card-issuing financial institutions can decide whether to issue fraud-resistant chip and PIN cards. Were the FTC required to enforce safeguard standards for credit and debit card data based on the Guidelines’ model, it would be imposing obligations on the entities with the least ability to ensure that they were carried out.

Finally, it is important to note that nonbanks, although not covered by the Safeguards Rule, are subject to the FTC’s general authority under Section 5 of the FTC Act to prohibit unfair or deceptive practices. The FTC has used this authority to prosecute dozens of nonbanks for engaging in the same practices proscribed by the Safeguards Rule, i.e., failing to take reasonable measures to protect consumers’ personally identifiable information.¹⁶ Thus, it is unclear what

¹⁴ See 16 C.F.R. Parts 681.1(b)(4), (5) (2009) (effective until February 11, 2013) (referring to 15 U.S.C.A. § 1691a(r)(5) (the Equal Credit Opportunity Act), which defines “creditor” as, among other things, “any person who regularly extends, renews, or continues credit,” and defines “credit” as “the right granted by a creditor to a debtor to... *purchase property or services and defer payment therefor*”) (emphasis added).

¹⁵ Red Flag Program Clarification Act of 2010, Pub. L. 111-319, § 2 (2010).

¹⁶ See, e.g., *FTC v. Wyndham Worldwide Corp., et al.*, No. CV 12-1365-PHX-PGR, in the U.S. District Court for the District of Arizona (2012); *In the Matter of Fandango, LLC*, Matter Number 132 3089 (2014); *In the Matter of Cbr Systems, Inc.*, Matter Number: 112 3120 (2013); *In the Matter of Dave & Buster’s, Inc.*, Matter Number 082 3153

additional benefit to the public would gain by subjecting nonbanks to specific requirements of the Guidelines.

As noted earlier, when issuing the GLBA rules, including the Safeguards Rule, the FTC specifically considered whether the rules should apply to retailers that accept bank-issued credit cards but do not extend credit themselves. The FTC correctly concluded that to do so would constitute a significant expansion of the FTC's authority to encompass the regulation of any transaction involving acceptance of a payment, whether cash, cards, checks or otherwise.

(2010); *In the Matter of CVS Caremark Corp.*, Matter Number: 072-3119 (2009); *In the Matter of Gencia Corp. and Compgeeks.com d/b/a computer Geeks Discount Outlet and Geeks.com*, Matter Number: 082 3113 (2009); *In the Matter of TJX Companies*, Matter Number: 072-3055 (2008); *In the Matter of Life is good, Inc. and Life is good Retail, Inc.*, Matter Number: 0723046 (2008); *U.S. v. ValueClick, Inc., et al.*, No. CV 08-01711, in the U.S. District Court for the Central District of California (2008); *In the Matter of Guidelines Software, Inc.*, Matter Number: 062 3057 (2007); *In the Matter of CardSystems Solutions, Inc.*, Matter Number: 052 3148 (2006); *In the Matter of DSW Inc.*, Matter Number: 052 3096 (2006); *In the Matter of BJ's Wholesale Club, Inc.*, Matter Number: 042 3160 (2005); *In the Matter of Petco Animal Supplies, Inc.*, Matter Number: 0323221 (2005); *In the Matter of Guess?, Inc. and Guess.com, Inc.*, Matter Number: 022 3260 (2003). These actions are in addition to those that the FTC has brought under the GLBA Safeguards Rule and/or the Consumer Information Disposal Rule. See, e.g., *U.S. v. PLS Financial Services, Inc., et al.*, Case No. 1:12-cv-08334, in the U.S. District Court for the Northern District of Illinois, Eastern Division (2012); *In the Matter of James B. Nutter & Company*, Matter Number: 0723108 (2009); *In the Matter of Premier Capital Lending*, Matter Number: 072 3004 (2008); *U.S. v. American United Mortgage Co.*, Civil Action No. 07C 7064, in the U.S. District Court for the Northern District of Illinois, Eastern Division (2007); *In the Matter of Nations Title Agency, Inc., et al.*, Matter Number: 052 3117 (2006).

Mr. BURGESS. The Chair thanks the gentleman.

The Chair now recognizes Ms. Moy. Five minutes for your opening statement, please.

STATEMENT OF LAURA MOY

Ms. MOY. Thank you. Good morning, Dr. Burgess, Ranking Member Schakowsky, distinguished members of the subcommittee. Thank you for your shared commitment to addressing data security and data breaches, and for the opportunity to testify on this important issue.

Consumers today share tremendous amounts of information about themselves. Consumers benefit from sharing information, but they can also be harmed if that information is compromised. For that reason, 47 States, and the District of Columbia, all currently have data breach laws on the books, and several States have specific data security laws. Many States also use general consumer protection provisions to enforce privacy and security.

To preserve strong State standards, and the ability to protect protections to the needs of their own residents, a Federal law should set a floor for disparate State laws, and not a ceiling. But, in the even that Congress seriously considers broad preemption, the new Federal standard should strengthen, or at least preserve, import protections that consumers currently enjoy. This bill, however, would weaken consumer protections in a number of key ways. These concerns must be addressed, and if they are not addressed, it would be better for privacy to pass no bill than to pass this bill as currently drafted. I will highlight five particular concerns.

First, the bill's definition of personal information is too narrow. The bill threatens to weaken existing protections by eliminating State laws covering information that falls outside of its narrow terms. For example, health information, as others have mentioned, falls outside this bill's definition of personal information. As a result, passing this bill would mean eliminating breach notification coverage of that information in Florida, Texas, and seven other States.

Second, this bill would condition breach notification on a narrow financial harm trigger. Data breaches may lead to a number of serious harms beyond merely those that are financial in nature, one reason why seven States and the District of Columbia have no harm trigger at all, and why triggers in another 26 States are not specifically financial in nature.

Third, the bill's general reasonableness security standard would replace the more specific security standard set forth in many State laws, and the FCC's rules implementing the Communications Act. Some States have specific data security standards in place, and the FCC's CPNI rules require carriers to train personnel on CPNI, have an express disciplinary process in place for abuses, and certify on an annual basis that they are in compliance with the rules. This bill threatens to eliminate these carefully designed security requirements, replacing them with a general reasonableness standard.

Fourth, this bill would supersede important provisions of the Communications Act that protect telecommunications, cable, and satellite customers. Consumers rely on the Communications Act,

and the FCC's implementation of it, to protect the very sensitive information that they cannot avoid sharing with the gatekeepers of communications networks. But this bill threatens to replace those protections with weaker standards. In addition, this bill would eliminate protections for the viewing histories of cable and satellite subscribers that fall outside the bill's definition of personal information. The proposed reduction of FCC authority could not come at a worse time for consumers, right as the FCC is poised to apply its Title 2 authority over data security and breach notification to broadband.

The bill strives to eliminate FCC authority only insofar as it relates to information security or breach notification, while preserving the FCC's authority to set privacy controls. But privacy rules that give consumers the right to control their information are of greatly diminished value when there are no security standards to protect against unauthorized access.

Fifth, the bill could eliminate a wide range of existing consumer protections that may be used to enforce both privacy and data security. The bill is designed to preempt State law and supersede the Communications Act only with respect to information security and breach notification, but in practice it would be exceedingly difficult to draw the line between information security and breach notification on the one hand, and privacy and general consumer protection on the other.

We are not unequivocally opposed to the idea of Federal data security and breach notification legislation, but any such legislation must strike a careful balance between preempting existing laws and providing consumers with new protections. The draft Data Security and Breach Notification Act of 2015 falls short of that balance, but we at the Open Technology Institute do appreciate your commitment to addressing these issues, and we hope to work with you to strengthen the bill and strike a better balance as it moves forward.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Moy follows:]



Statement of Laura Moy
Senior Policy Counsel
New America's Open Technology Institute

Before the House of Representatives Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on
Discussion Draft of H.R. ___, Data Security and Breach Notification Act of
2015

March 18, 2015

Chairman Burgess, Ranking Member Schakowsky, and Members of the
Subcommittee:

Thank you for working to address data security and data breaches, and for the opportunity to testify on this important issue. I represent New America's Open Technology Institute (OTI), where I am Senior Policy Counsel specializing in consumer privacy, telecommunications, and copyright. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is New America's program dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks.

I have been invited here today to present my views as a consumer and privacy advocate. Consumers today share tremendous amounts of highly personal information with a wide range of actors both online and offline. Consumers can benefit enormously from sharing personal information, but distribution of personal information beyond its original purpose can lead to

financial, emotional, or even physical harms. In recognition of those possible harms, 47 states and the District of Columbia currently have data breach laws on the books, several states have specific data security laws, and many states also use general consumer protection provisions to enforce privacy and security.

To preserve strong state standards and states' ability to adapt protections to best meet the needs of their own residents, a federal data security and breach notification law should merely set a *floor* for disparate state laws – not a ceiling. But the draft Data Security and Breach Notification Act would eliminate many state laws – as well as some provisions of federal law – that provide stronger consumer protections, in the interest of establishing a single standard nationwide.

In the event that Congress is seriously considering such broad preemption, the new federal standard should strengthen, or at the very least preserve, important protections that consumers currently enjoy. This bill, however, would *weaken* consumer protections in a number of ways, and eliminate protections altogether for some categories of personal information. We are particularly concerned that:

- 1) the bill's definition of personal information is too narrow,
- 2) it would condition breach notification on a narrow financial harm trigger,
- 3) it would replace strong existing information security protections with a less specific "reasonableness" standard,
- 4) it would supersede important provisions of the Communications Act, and
- 5) it could invalidate a wide range of privacy laws that do not deal exclusively with information security and data breach.¹

¹ These are many of the same concerns that we voiced in a February 5, 2015 letter to Senators Thune and Nelson. Other signatories to the letter were Center for Democracy & Technology, Center for Digital Democracy, Consumer Action, Consumer Federation of America, Consumer Watchdog, National Consumers

1. The Bill Would Weaken or Eliminate Protections for Information that Falls Outside the Bill's Narrow Definition of "Personal Information"

First, many privacy and consumer advocates are concerned that this bill defines "personal information" too narrowly. This narrow definition, in combination with the preemption provision, would weaken existing protections by eliminating state-level protections for types of information that fall outside of its narrow terms.

For example, under Florida's data security and breach notification law, the definition of personal information includes an email address and password combination, information that could be used to compromise all of an individual's private emails, as well as information in any account that uses an email address as a login ID, because many consumers recycle the same password across multiple accounts.² Florida's law also protects a wide range of information about physical and mental health, medical history, and insurance,³ as do the state laws of California,⁴ Missouri,⁵ New Hampshire,⁶ North Dakota,⁷ Texas,⁸ Virginia,⁹

League, Public Knowledge, Privacy Rights Clearinghouse, and U.S. PIRG. Letter to Senators John Thune and Bill Nelson, Feb. 5, 2015, <https://cdt.org/insight/letter-to-senate-on-data-breach-legislative-proposals/>.

² Fla. Stat. § 501.171.

³ Health care and insurance providers are not included in the definition of "covered entity" under this bill; thus, the bill would not preempt laws crafted narrowly to govern data security and breach notification with respect to those entities. However, there are entities other than health care and insurance providers that collect health-related information, and this bill would preempt state laws that cover health information and extend to those entities, without providing comparable coverage under the new federal standard.

⁴ Cal. Civ. Code § 1798.29.

⁵ Mo. Rev. Stat. § 407.1500.

⁶ N.H. Rev. Stat. Ann. § 359-C:20.

⁷ N.D. Cent. Code § 51-30-01, 51-30-02.

⁸ Tex. Bus. & Com. Code § 521.002.

⁹ Va. Code Ann. 32.1-127.1C.

and — beginning July 1 — Hawaii and Wyoming.¹⁰ Compromised medical information is often a key element in medical identity theft, a rising trend.¹¹ North Dakota's breach notification law protects electronic signature, date of birth, and mother's maiden name, pieces of information that could be used to verify identity for the purpose of fraudulently creating or logging into an online or financial account.¹²

However, because health and medical information, email/password combinations, and electronic signatures do not fall within this bill's definition of "personal information," this bill does not protect that information, nor protect against the serious harms that breach of that information could lead to. At the same time, this bill would eliminate the state laws that *do* protect that information, substantially weakening the protections that consumers currently enjoy. In other words, today in seven states, companies are universally required to protect health information from data breach, and if this bill passes, consumers in those states will lose that protection.

Relatedly, we are concerned that this bill does not provide the necessary flexibility with respect to personal information to account for changing technology and information practices. Flexibility could be built in by limiting preemption in a manner that allows states to continue to establish standards for categories of information that fall outside the scope of this bill as, for example,

¹⁰ See Elizabeth Snell, *Wyoming Security Breach Notification Bill Includes Health Information*, Health IT Security (Feb. 23, 2015), <http://healthitsecurity.com/2015/02/23/wyo-security-breach-notification-bill-includes-health-data/>.

¹¹ Dan Munro, *New Study Says Over 2 Million Americans Are Victims Of Medical Identity Theft*, Forbes (Feb. 23, 2015), <http://www.forbes.com/sites/danmunro/2015/02/23/new-study-says-over-2-million-americans-are-victims-of-medical-identity-theft/>.

¹² N.D. Cent. Code § 51-30.

Hawaii and Wyoming did just this year.¹³ Flexibility could also be created by providing agency rulemaking authority to enable the FTC to redefine personal information to include new categories of information to adapt to changing technology.

2. The Bill Would Weaken Existing Protections by Tying Breach Notification to a “Harm Trigger”

Second, we are concerned that this bill weakens existing consumer protections because it allows covered entities to avoid notifying customers of a breach if they determine that there is no risk of financial harm. Harm triggers are problematic, because it is often very difficult to trace a specific harm to a particular breach, and because after a breach has occurred, spending time and resources on the completion of a risk analysis can delay notification. Moreover, the breached entity may not have the necessary information—or the appropriate incentive—to effectively judge the risk of harm created by the breach.

In addition, the trigger standard set forth in the bill is far too narrow, as it ignores the many non-financial harms that can result from a data breach. For example, an individual could suffer harm to dignity if he stored nude photos in the cloud and those photos were compromised. If an individual’s personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some circumstances, breach could even lead to physical harm. For example, the fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life.

Many state laws recognize these various types of non-financial harms. Accordingly, many states require breach notification regardless of a risk assessment, or, if they do include some kind of harm trigger, take into account other types of harms beyond the strictly financial. For example, there is no harm

¹³ See *supra* note 10.

trigger at all in California,¹⁴ Illinois,¹⁵ Minnesota,¹⁶ Nevada,¹⁷ New York,¹⁸ North Dakota,¹⁹ Texas,²⁰ and the District of Columbia.²¹ The majority of states have a trigger that turns on “harm,” “misuse,” “loss,” or “injury” not specifically financial in nature: Alaska,²² Arkansas,²³ Colorado,²⁴ Connecticut,²⁵ Delaware,²⁶ Georgia, Hawaii,²⁷ Idaho,²⁸ Louisiana,²⁹ Maine,³⁰ Maryland,³¹ Michigan,³² Mississippi,³³ Montana,³⁴ Nebraska,³⁵ New Hampshire,³⁶ New Jersey,³⁷ North Carolina,³⁸ Oregon,³⁹ Pennsylvania,⁴⁰ South Carolina,⁴¹ Tennessee,⁴² Utah,⁴³ Vermont,⁴⁴ Washington,⁴⁵ and Wyoming.⁴⁶

¹⁴ Cal. Civ. Code § 1798.29.

¹⁵ 815 Ill. Comp. Stat. § 530/10.

¹⁶ Minn. Stat. § 325E.61.

¹⁷ Nev. Rev. Stat. § 603A.220.

¹⁸ N.Y. General Business Laws § 899aa.

¹⁹ N.D. Cent. Code § 51-30-01, 51-30-02.

²⁰ Tex. Bus. & Com. Code § 521.053.

²¹ D.C. Code § 28-3852.

²² Alaska Stat. § 45.48.010.

²³ Ark. Code Ann. § 4-110-105.

²⁴ Colo. Rev. Stat. § 6-1-716.

²⁵ Conn. Gen. Stat. § 36a-701b.

²⁶ Del. Code tit. 6, § 12B-102.

²⁷ Haw. Rev. Stat. § 487N-1.

²⁸ Idaho Code Ann. § 28-51-105.

²⁹ La. Rev. Stat. Ann. § 51:3074.

³⁰ Me. Rev. Stat. Ann. tit. 10, § 1348.

³¹ Md. Code Ann. Com. Law § 14-3504.

³² Mich. Comp. Laws § 445.72.

³³ Miss. Code Ann. § 75-24-29.

³⁴ Mon. Code Ann. § 30-14-1704.

³⁵ Neb. Rev. Stat. § 87-803.

³⁶ N.H. Rev. Stat. Ann. § 359-C:20.

³⁷ N.J. Stat. Ann. § C.56:8-163.

³⁸ N.C. Gen. Stat. § 75-61; *see* N.C. Gen. Stat § 75-65.

³⁹ Or. Rev. Stat. § 646A.604.

⁴⁰ 73 Pa. Stat. Ann. § 2302.

⁴¹ S.C. Code Ann. § 1-11-490.

⁴² Tenn. Code Ann. § 47-18-2107.

This bill constitutes a step backwards for many consumers in the above-named 33 states and the District of Columbia. The bill should leave room for states to require notification even in circumstances where the harm is not clear or is not financial in nature. Barring that, at the very least the bill's trigger provision should be as inclusive as the most inclusive state-level triggers.

3. The Bill's "Reasonableness" Security Standard Would Eliminate More Specific Data Security Protections Without Offering Consumers New Protections

Third, we are concerned that the bill's general "reasonableness" security standard, in combination with preemption provisions, would replace the more specific security standards set forth in many state laws and the FCC's rules implementing the Communications Act.

For example, Nevada's data security law requires covered entities that accept payment cards to abide by the Payment Card Industry Data Security Standard.⁴⁷ The data security regulations of Massachusetts set forth a number of very specific data security requirements.⁴⁸ The Communications Act grants the FCC rulemaking authority with respect to the information of telecommunications, cable, and satellite subscribers. The FCC's robust rules promulgated under that authority require telecommunications carriers to, among other things, train personnel on customer proprietary network information (CPNI), have an express disciplinary process in place for abuses, and annually certify that they are in

⁴³ Utah Code Ann. § 13-44-202.

⁴⁴ Vt. Stat. Ann. § 2435.

⁴⁵ Wash. Rev. Code § 19.255.010.

⁴⁶ Wyo. Stat. Ann. § 40-12-502.

⁴⁷ Nev. Rev. Stat. § 603A.215.

⁴⁸ 201 Mass. Code Regs. 17.03-17.04.

compliance with the CPNI rules.⁴⁹ The specific requirements of states such as Nevada and Massachusetts, along with the specific data security requirements imposed by the FCC, would all be eliminated by this bill and replaced with the less specific “reasonableness” standard.

Perhaps more significant, consumers residing in states that have no data security law on the books would not gain any new protections for their personal information from this bill, beyond what is already required under § 5 of the Federal Trade Commission Act as interpreted by the FTC. Since 2002, the FTC has brought over fifty cases against companies for failing to implement security measures that are “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.”⁵⁰ The standard in this bill is the same as the standard that is already vigorously enforced by the FTC under its existing authority.

Because this bill would eliminate detailed state- and communications-sector-specific data security protections to institute a federal standard that does not offer anything new to protect consumers, this bill could actually water down data security requirements. It would be better for consumers if the bill set a nationwide floor at reasonable security, but allowed states and the FCC, at their discretion, to develop more specific requirements beyond that standard, as circumstances demand.

⁴⁹ 47 C.F.R. 64.2009.

⁵⁰ Federal Trade Commission, Commission Statement Marking the FTC’s 50th Data Security Settlement at 1 (Jan. 31, 2014), <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.

4. The Bill Would Eliminate Important Communications Act Protections for Telecommunications, Cable, and Satellite Customers

Fourth, we are concerned that this bill would supersede important provisions of the Communications Act that protect the personal information of telecommunications, cable, and satellite customers. Under this bill, some of the information currently covered under the Communications Act would no longer be protected, and the information that would still be covered would be covered by lesser standards.

The Communications Act protects telecommunications subscribers' CPNI, which includes virtually all information about a customer's use of the service.⁵¹ It also protects cable⁵² and satellite⁵³ subscribers' information, including their viewing histories. But as with email login information and health records, this bill is too narrow to cover all CPNI, and it would not protect cable and satellite viewing histories at all, so data security and breach notification protections for those types of information would simply be eliminated.

The proposed reduction of the FCC's CPNI authority could not come at a worse time for consumers, because the Federal Communications Commission has just voted to reclassify broadband Internet access as a telecommunications service under Title II of the Communications Act, enabling it to apply its CPNI authority to broadband Internet access providers. Applied to broadband, the CPNI provisions will require Internet service providers to safeguard information about use of the service that, as gatekeepers, they are in a unique position to collect: information such as what sites an Internet user visits and how often, with whom she chats online, what apps she uses, what wireless devices she owns, and even the location of those devices.

⁵¹ 47 U.S.C. § 222.

⁵² 47 U.S.C. § 551.

⁵³ 47 U.S.C. § 338.

This bill strives to leave intact the FCC's authority to set privacy controls for the personal information of telecommunications, cable, and satellite customers. But privacy controls are of greatly diminished value when there are no information security standards for the information at stake. For example, under its Title II authority the FCC may clarify that a broadband provider has to obtain a customer's explicit opt-in consent before sharing his browsing history with a third party. In a situation like the recently publicized "permacookie," the FCC could find Verizon in violation of consent requirements for failing to get customers' permission before attaching unique identifiers to their Internet traffic that enabled third parties to learn information about their browsing histories. But under this bill the agency could not impose any security requirements on Verizon to protect customers' browsing histories in the future.

Moreover, as discussed further below, we are concerned that it will be difficult in practice to distinguish information security from traditional privacy, and that as a result this bill would in fact preempt the Communications Act's privacy provisions more broadly.

The consumer protections provided by the Communications Act are of critical importance to consumers, and appropriately overseen by an agency with decades of experience regulating entities that serve as gatekeepers to essential communications networks. This bill threatens to eliminate core components of those protections.

5. The Bill Would Threaten a Wide Range of Privacy and General Consumer Protection Laws

Fifth, we are very concerned that the preemption language in the bill as currently drafted could eliminate a wide range of existing consumer protections under state law and the Communications Act, including many protections that may be used to enforce data security, but that are also used to provide other consumer or privacy protections. This bill is designed to preempt state law and

supersede the Communications Act only with respect to information security and breach notification,⁵⁴ but as a practical matter, it will be exceedingly difficult to draw the line between information security and breach notification on the one hand, and privacy and general consumer protection on the other.

We generally think of “privacy” as having to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information “security” refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject’s privacy (his right to control how his information is used or shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Many laws that protect consumers’ personal information could thus be thought of simultaneously in terms of both privacy and security. For example, in California, the Song-Beverly Credit Card Act prohibits retailers from recording any “personal identification information” of a credit cardholder in the course of a transaction.⁵⁵ In Connecticut, Section 42-470 of the General Statutes prohibits the public posting of any individual’s Social Security number.⁵⁶ These laws could be framed as both privacy and data security laws. State-level general consumer protection laws prohibiting unfair and deceptive trade practices (sometimes known as “mini-FTC Acts”) are also used to enforce both privacy and security.

Because each of these examples arguably constitutes a “law . . . relating to or with respect to the security of data in electronic form or notification following

⁵⁴ The bill would preempt state law “relating to or with respect to the security of data in electronic form or notification following a breach of security.” It would supersede several sections of the Communications Act insofar as they “apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information.”

⁵⁵ Cal. Civ. Code § 1747.08.

⁵⁶ Conn. Gen. Stat. § 42-470.

a breach of security” consistent with the legislation’s preemption language, consumer and privacy advocates are very concerned that this bill could unintentionally eliminate these and other important state-level consumer protections that are not strictly data security protections, but that have a data security aspect.

Similarly, we are concerned that this bill could broadly eliminate the privacy protections of the Communications Act. The bill would supersede the Communications Act insofar as the referenced provisions “apply to covered entities with respect to securing information in electronic form from unauthorized access.” It is unclear how this would apply to the FCC’s privacy rules, such as the rules that determine when CPNI access is authorized, and when it is not. For example, the FCC’s rules require carriers to get customers’ express opt-in consent before sharing CPNI with third parties. Complying with the consent rules could thus be considered “securing information . . . from unauthorized access,” while sharing information without the appropriate consent could be considered “unauthorized access,” or failing to “secure information . . . from unauthorized access.” In the Verizon permacookie example discussed briefly above, the FCC could find Verizon in violation of CPNI consent requirements for attaching unique identifiers’ to its customers’ web traffic, but Verizon could push back and argue that it did not foresee those identifiers being used by third parties for that purpose, and that the issue was therefore one of information security, rather than privacy.

In light of consumer protections that implicate both data security and privacy, such as California’s Song-Beverly Credit Card Act and the FCC’s CPNI rules, it is important for the subcommittee to reconsider the scope of preemption in this bill to avoid invalidating numerous privacy protections.

Conclusion

We are not unequivocally opposed to the idea of federal data security and breach notification legislation, but any such legislation must strike a careful balance between preempting existing laws and providing consumers with new protections. The draft Data Security and Breach Notification Act of 2015 falls short of that balance. However, the Open Technology Institute appreciates your commitment to consumer privacy, and we look forward to working with you to strengthen this bill and strike a better balance as it moves forward. I am grateful for the Subcommittee's attention to this important issue, and for the opportunity to present this testimony.

Mr. BURGESS. Thank you for your testimony.

Ms. Weinman, welcome to the subcommittee. You are now recognized for 5 minutes for the purpose of an opening statement.

STATEMENT OF Yael WEINMAN

Ms. WEINMAN. Thank you. Chairman Burgess, Ranking Member Schakowsky, and members of the subcommittee, thank you for the opportunity to testify today. My name is Yael Weinman, and I am the Vice President for Global Privacy Policy and the General Counsel at the Information Technology Industry Council, known as ITI. Prior to joining ITI in 2013, I spent more than 10 years as an attorney at the Federal Trade Commission, most recently as an attorney advisor to Commissioner Julie Brill.

The 60 technology companies that ITI represents are leaders and innovators in the information and communications technology sector. These are companies that are committed to the security of their customers' information. The reality remains, however, that while organizations race to keep up with hackers, these criminals attempt to stay one step ahead. And when a network is compromised, and personal information has been breached, individuals may be at risk of identity theft or financial fraud.

Consumers can take steps to protect themselves from identity theft or other financial fraud following a data breach. Federal breach notification legislation would put consumers in the best possible position to do so. In the written testimony I provided to you in advance of this hearing, I included the set of nine principles that ITI recommends be included in Federal breach notification legislation. The draft legislation that is the subject of this hearing reflects a number of these important principles. I highlight three.

First, the legislation preempts the existing patchwork in the United States of 51 different regimes. That is 47 States and four territories. Such preemption is critical in order to streamline notices and avoid consumer confusion. Second, the legislation's timeline for notification recognizes that notification can only take place once an organization determines the scope of the data breach, and has remedied vulnerabilities. The timeline included in the draft legislation also permits the necessary flexibility to enable companies to delay notification at the request of law enforcement. Third, the legislation does not require notification if data is unusable, recognizing that power security tools have been developed that avoid risks if data has been compromised.

ITI appreciates how these three important elements are incorporated into the draft legislation. Greater clarity and discussion is needed, however, in a number of areas, and I highlight three today.

First, the description of the level of risk, and the potential ensuing harm that would trigger the notification, appears to be broad. The threshold of reasonable risk, combined with the phrase economic loss or economic harm could lead to over-notification. It is unclear how economic loss or economic harm is being distinguished from the phrase financial fraud that also appears in the text. Year after year, identity theft tops the list of consumer complaints reported to the FTC, and identity theft or financial fraud are the appropriate triggers for providing consumer notice. And, upon notifi-

cation, consumers can then take the necessary steps to protect themselves.

Second, with regard to the timing of notification, as currently written, the timeline for a covered entity to notify consumers if a third party suffered a data breach is unclear. The third party needs to remedy vulnerabilities and restore its systems before the covered entity provides notice. The draft should be clarified that the third party will be given the opportunity to restore its system prior to the point in time that the covered entity is required to provide notice to consumers.

Third, the maximum penalty amounts set in the draft legislation are high, \$2.5 million maximum for each violation of the data security section, and a \$2.5 million maximum for notice related violations arising from a single incident. These amounts appear punitive, and do not seem to reflect that an organization that suffered a data breach, in most cases, is the victim itself of criminal hackers.

As ITI and its member companies continue to study the draft, and as we gather feedback, we look forward to sharing that with members of the committee. Thank you, and I am happy to answer any questions.

[The prepared statement of Ms. Weinman follows:]



Information Technology
Industry Council

Written Testimony of
Yael Weinman

Vice President, Global Privacy Policy and General Counsel
Information Technology Industry Council (ITI)

Before the
Subcommittee on Commerce, Manufacturing, and Trade

U.S. House Committee on Energy & Commerce

Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015

March 18, 2015



Information Technology Industry Council

Summary of Testimony of Yael Weinman

Federal data breach notification legislation offers the opportunity to develop a single uniform standard, and should achieve the important goals of reducing consumer confusion, enabling faster consumer notification, and avoiding over-notification and consumer desensitization. ITI developed principles containing the elements a data breach notification bill must include to achieve these goals. We note that the *Data Security and Breach Notification Act of 2015* includes a number of these critical elements in that it: (a) preempts the patchwork of 51 breach notification regimes; (b) recognizes that consumers want clarity and certainty in their notices; (c) recognizes that notification can only take place once an organization determines the scope of any data breach and has remedied vulnerabilities; (d) allows for flexibility in notification, permitting companies to heed law enforcement requests to delay notification; (e) recognizes the importance of avoiding over notification; (f) recognizes how businesses communicate with their customers in today's economy and permits flexibility in how notification is provided; (g) recognizes that data may be rendered unusable by certain security tools; (h) recognizes the reality of third-party business relationships; and (i) avoids subjecting certain industries to duplicative regulation when they are subject to existing sector-specific regimes.

Certain aspects of the draft legislation would benefit from greater clarity and further consideration. In particular, the threshold of "reasonable risk" combined with the phrase "economic loss or economic harm" could lead to over-notification. Another area that would benefit from greater clarity is the timeline for notification by a covered entity if the data breach was suffered by a third-party entity. As written, it is unclear whether the covered entity's notification requirement commences only when the third-party entity has had the opportunity to restore the integrity of its system. We also note that the defined term "breach of security" in the draft bill is not clear in that it includes a reference to the compromise of "security" thus creating circularity within the definition. In addition, the use of the definition could have negative unintended consequences in foreign jurisdictions that are considering imposing problematic cybersecurity requirements on the tech sector. We further note that the penalties authorized in the draft legislation are elevated and thus unfairly punitive for an organization that is itself victim of a crime.



Information Technology Industry Council

Written Testimony of:

Yael Weinman

VP, Global Privacy Policy and General Counsel

Information Technology Industry Council (ITI)

Before the:

Subcommittee on Commerce, Manufacturing, and Trade

U.S. House Committee on Energy & Commerce

Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015

March 18, 2015

Chairman Burgess, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Yael Weinman and I am the Vice President for Global Privacy Policy and the General Counsel at the Information Technology Industry Council, also known as ITI. Prior to joining ITI, I spent more than 10 years as an attorney at the Federal Trade Commission, most recently as an Attorney Advisor to Commissioner Julie Brill.

ITI is the global voice of the technology sector. The 60 companies ITI represents—the majority based in the United States—are leaders and innovators in the information and communications technology (ICT) sector, including in hardware, software, and services. Our companies are at the forefront of developing the technologies that protect our networks. When a data breach occurs, however, there needs to be a streamlined process that helps guide how consumers are informed in cases when there is a significant risk of identity theft or financial harm resulting from the breach of personally identifiable information.

While companies and financial institutions invest tremendous resources in defending their infrastructures and protecting their customers' information, it is an ongoing virtual arms race. Organizations race to keep up with hackers while the criminals scheme to stay one step ahead. Unfortunately, it is no longer a matter of *if*, but a matter of *when*, a criminal hacker will target an

organization. And when certain information about individuals is exposed, those consumers may be at a significant risk of identity theft or other financial fraud.

As a result of this troubling landscape, over the years legislatures across the country enacted data breach notification regimes. Currently, there are 51 such regimes—in 47 states and four U.S. territories.¹ Consumers across the country have received notifications pursuant to these laws. I have received more than one such notice myself, and I imagine some of you may have as well.

As a result of this patchwork, the current scope of legal obligations in the United States following a data breach is complex. Each of the 51 state and territory breach notification laws vary by some degree, and some directly conflict with one another. There are significant variances among these state and territory laws, including the timeline for notification, what circumstances give rise to a notification requirement, how a notification should be effectuated, and what information should be included in a notification. Federal data breach notification legislation offers the opportunity to streamline these requirements into a single, uniform standard.

Federal data breach notification legislation should achieve the important goals of reducing consumer confusion, enabling faster consumer notification, and avoiding over-notification and consumer desensitization. ITI developed principles containing the elements a data breach notification bill must include to achieve these goals. The principals are attached to this testimony as Exhibit A. The *Data Security and Breach Notification Act of 2015* reflects several of these principles and offers a certain level of regulatory clarity and certainty, which is critical for businesses—like ITI member companies—that devote tremendous resources to legal compliance:

¹ The District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands each adopted a data breach notification law. New Mexico, South Dakota, and Alabama have not yet enacted breach notification laws.

- The draft bill preempts the patchwork of 51 breach notification regimes. Preemption is critical in order to streamline the data breach notification regime in place today. Without preemption, however, the bill would further muddy the unclear waters and add another layer of complexity to the data breach response process by adding a 52nd law to the existing patchwork. By creating a single breach notification regime, consumers will experience consistency across notices, thereby ensuring notices are more easily understood, and companies will save response time by not running through 51 different checklists before sending a notification.
- The bill recognizes that consumers want clarity and certainty in their notices, and that they expect a company who suffers a breach to attempt to mitigate further harm. The bill recognizes that notification can only take place once an organization determines the scope of any data breach and has remedied vulnerabilities. Providing notice of a breach while a system remains vulnerable risks further attacks, potentially making consumer information more vulnerable. The bill also allows for flexibility in notification, permitting companies to heed law enforcement requests to delay notification to investigate the incident or pursue bad actors engaged in criminal activities.
- The bill recognizes the importance of avoiding over-notification; the definition of “personal information” in the draft bill is appropriately limited to data, which, if obtained by a criminal, could result in concrete financial harms.
- The bill recognizes how businesses communicate with their customers in today’s economy and permits flexibility in how notices occur. If a consumer typically engages with a company via email or other electronic means, then those would be permitted methods of providing notification. This is highly important, as consumers may not expect a written letter containing such a notice if they have previously only communicated with such companies electronically. Consumers and companies should have the flexibility to choose how to send and receive important notifications.

- The bill recognizes that data may be rendered unusable by certain security tools. Our companies are at the forefront of developing and utilizing the technologies to protect our networks and data. If data is unusable or unreadable notification is unnecessary.
- The bill recognizes the reality of third-party business relationships. Many organizations contract with third parties to maintain or process personal information. Consumers may be unaware of these third-party relationships and requiring a notification from the unknown third party to the consumer may create unnecessary confusion.
- The bill recognizes existing statutory regulatory frameworks and avoids subjecting certain industries to duplicative regulation when they are subject to existing sector-specific regimes.

ITI recognizes that many of the principles it has developed on data breach notification are reflected in the draft bill. However, certain aspects of the draft bill raise concerns in that they do not provide sufficient clarity as to what is to be expected of organizations—and such lack of clarity could be detrimental to consumers. Without clarity and certainty of what is required by law, companies will err on the side of caution to avoid being on the wrong side of a Federal law, resulting in over-notification to consumers and the desensitization of consumers to these notices.

One area where greater clarity is necessary is the description of the risk threshold that triggers consumer notification. ITI appreciates that the bill ties the unauthorized acquisition of “personal information” to the risk trigger. However, we are concerned that the threshold of “reasonable risk,”—which is lower than the “significant risk” threshold recommended in ITI’s data breach notification principles—combined with the term “economic loss or harm” will inevitably lead to over-notification. It is unclear what is meant by “economic loss or harm” and how that category is distinguished from the phrase “financial fraud.” The purpose of the bill is to enable consumers to take steps to protect themselves from identity theft and financial harm that can be perpetrated

by criminals who have gained access to certain personal information. Accordingly, we believe that tying the level of risk to “identity theft and financial harm” captures the scope of activities that consumers need to protect themselves from following a data breach. Accordingly, we urge you to consider eliminating the phrase “economic loss or harm” from the bill.

Another area that would benefit from greater clarity is the timeline for consumer notification following a data breach suffered by a third-party entity. The bill requires third-party entities to promptly notify the “covered entity.” It is then unclear when the covered entity is required to notify consumers. When the covered entity itself suffers a data breach, notification occurs once the covered entity determines the scope of the breach and restores the integrity of its systems. As currently drafted, it could be construed that a covered entity, upon notification by the third-party of a breach, would need to notify its customers prior to the point in time when the third-party has determined the scope of the breach and restored the integrity of its systems. Accordingly, we recommend the Committee amend subsection 3(b)(1)(B) to read:

Upon receiving notification from a third-party entity under subparagraph (A), a covered entity shall, *after the third-party entity has taken the necessary measures to restore the reasonable integrity, security, and confidentiality of the data system*, provide notification as required under subsection (a), unless it is agreed in writing that the third-party entity will provide such notification on behalf of the covered entity subject to the requirements of subsection (d)(3).

We also urge the Committee to eliminate the definition of “breach of security.” First, the definition is confusing in that the meaning of a key phrase within it—“compromise of the security”—is itself unclear. In addition, this broad definition of “breach of security” could have negative consequences on our advocacy in foreign markets. A number of foreign governments are contemplating imposing problematic cybersecurity requirements on the technology sector, sometimes not for legitimate security reasons but rather to promote their own domestic industries. For the Congress to enact a law with a broad definition could empower other

countries to adopt the same definition with troubling results. The critical elements of this bill are to notify consumers within an appropriate period of time after the unauthorized acquisition of certain personal information that will likely result in certain harms—we believe defining a “breach of security” is not critical to this functionality. Given the potential for harmful, unintended consequences globally, we urge the Committee to eliminate this unnecessary definition, and directly tie personal information to the specific harms within subsection 3(a)(1).

Finally, the bill permits civil penalties of up to \$2.5 million for each violation of section 2 (*Requirements for Information Security*) and up to \$2.5 million for all violations of section 3 (*Notification of Information Security Breach*) arising from a single incident. Most data breaches are the result of criminal acts, and therefore, breached entities are the victims of a crime. Organizations can and should do their part to protect consumer data from unauthorized access, but civil penalties that are five times higher than previous Congressional proposals are seemingly punitive in nature and thus not appropriate to impose on an organization that has been victimized by criminal hackers.

As ITI continues to gather feedback on the *Data Security and Breach Notification Act of 2015* from its member companies, we look forward to sharing that feedback with the Committee. Thank you again for the opportunity to testify today and I am happy to answer any questions you may have.



Exhibit A



Data Breach Notification Principles

The Information Technology Industry Council (ITI) strongly supports efforts to establish a commonsense, uniform national breach notification regime to help consumers when there is a significant risk of identity theft or financial harm. We are committed to working with Congress to enact meaningful legislation that establishes a national data breach notification process that is simple and consumer-driven. As the committees of jurisdiction in the House and Senate work to develop their respective bills, we urge Members to include the following key elements:

1. Federal Preemption. ITI supports the creation of a strong federal breach notification law. Effective federal preemption of the multitude of state notification laws will allow businesses to notify consumers more quickly when a breach of sensitive personal data occurs by easing the confusion and duplication that results from the current patchwork of competing, and often conflicting, state requirements. With almost every state now having enacted data breach notification laws, it is important that the role of the states be carefully defined in federal legislation.

2. Inaccessible, Unusable, Unreadable, or Indecipherable Data. Data may be unusable due to the absence of critical pieces, obfuscation, encryption, redaction, anonymization, or expiration by its own terms. Effective security practices and methods change over time and new technologies continue to evolve which enable data to be rendered unusable. An effective "unusable data" provision would make clear that notification is not required when there is a reasonable determination that data is rendered inaccessible, unusable, unreadable, or indecipherable. It is important that federal legislation not single out or give preference to one method of rendering data unusable as a means to avoid notification. Such action could create a false sense of security and create a compliance basement which may reduce the development and use of diverse and innovative security tools. ITI supports legislation that recognizes such technologies with technology-neutral and method-neutral language and that allows businesses to determine whether or not data may be used for the purposes of committing identity theft or financial harm.

3. Effective Harm-Based Trigger. Federal breach notification legislation must recognize the delicate balance between over- and under-notification with respect to when notices should be sent to consumers. ITI strongly believes notification should only be required after organizations determine the unauthorized acquisition of sensitive personal data could result in a significant risk of identity theft or financial harm. Expanding the types of harm to vague or subjective concepts such as "other unlawful conduct" creates confusion and will result in over-notification. Additionally, efforts to lower the threshold to a reasonable risk of identity theft or financial harm will expose consumers and businesses to the numerous costs associated with over-notification. Further, the definition of a data breach should clearly tie an "unauthorized acquisition of sensitive personal information" to the risk of identity theft or financial harm. Not all data breaches are nefarious nor do they create a risk to consumers. Failing to recognize this in the definition of a data breach would expose organizations to possible enforcement action by government entities, including state attorneys general, for unauthorized breaches, regardless of the risk of identity theft or financial harm.



4. Reasonable Scope of Legislation. The protection of consumer information across industries is a complex statutory and regulatory puzzle. It is important that federal breach notification legislation does not create unworkable and overlapping regulatory regimes for commercial and financial services industries. Entities that are already subject to any existing federal data breach requirements in a sector-specific law should continue to be required to comply with those laws and should not be subject to additional regimes.

5. Flexible Manner of Notification. Federal data breach notification requirements must accommodate both traditional companies that communicate with customers by mail, telephone, or fax and online companies that communicate predominantly through electronic communication (e.g., electronic mail). Consumers trust that companies will notify them in a manner that is consistent with previous communications and expect that will be done in an expedient and timely manner. A consumer receiving a telephone call from their email provider outlining a breach and urging action would be justifiably suspicious.

6. Third Party Requirements. Many organizations contract with third parties to maintain or process data containing personal information. Consumers may be unaware of these third-party relationships and requiring a notification from the third party to the consumer may create unnecessary confusion. In the event of a data breach of any third party system, the third party should be required to notify the consumer-facing company of the breach. The consumer-facing company and the third party should then have the flexibility to determine which entity should notify consumers. Additionally, legislation should not require notification of a broad range of third parties other than the consumer and credit reporting bureaus in the event of an actual or likely breach.

7. No Private Right of Action. An effective breach notification requirement and an efficient enforcement framework provides the best protection for consumers and will avoid unnecessary and frivolous litigation. Legislation should also prohibit the use of government regulatory enforcement action in private litigation asserting non-preempted state or other causes of action.

8. No Criminal Penalties. Most data breaches are the result of criminal acts, and therefore, breached entities are the victims of a crime. Organizations can and should do their part to protect consumer data from unauthorized access, but they should not be subject to criminal sanctions for being victimized by criminal hackers.

9. Discovery, Assessment, Mitigation, and Notice. Federal legislation must allow organizations to redress the vulnerability and conduct thorough investigations of suspected data breaches before notifying customers or government agencies. Unless the vulnerability is addressed prior to making the incident public, the organization and its customers are susceptible to further harm. Notifying customers will be counterproductive should the alleged breach prove false or if the breach does not create a risk of identity theft. A tremendous amount of forensics, decision-making, and legal work is required before ascertaining the nature and scope of a breach, assessing the risk of harm, and determining the appropriate form of notification. Recognizing the sophistications of today's hackers, and the challenging nature of a post-data breach forensic investigation, federal legislation must provide realistic, flexible, and workable time requirements, as well as recognize the need to cooperate with law enforcement in their criminal investigations.

Mr. BURGESS. The Chair thanks the gentlelady, thanks all the witnesses for your forthright testimony today. We will move into the question and answer portion of this panel. Recognize myself for 5 minutes for questions.

And, Mr. Leibowitz, if I could, let me start with you. You are familiar with the draft legislation before us. Do you think consumers would be more or less protected with respect to information held by telecom providers under this draft?

Mr. LEIBOWITZ. I think—look, my view is that consumers—if this bill were to pass tomorrow, be signed into law, consumers would be in a better position, and let me just tell you why I think that.

First of all, the, you know, the FTC, as the witnesses—both witnesses acknowledged in the previous panel, has been a leader, America's top consumer protection cop, including in the data security area, with more than 50 cases, and hundreds of investigations. There is an emerging consensus, and I think this is critically important, that the most appropriate way to protect personal information, and this is at the core of your bill, is with strong, but flexible, data security standards. It is not with prescriptive rules.

And there is also an ever-changing patchwork of State legislation. Now, I have seen legislation, when I was at the FTC, that sometimes took State AGs entirely out of the business of enforcing the law. You do not do that, and I think that is critically important, because you want State AGs to be a top cop here. And nobody wants to see any gaps in the legislation. I do not read this legislation as having any gaps, but we certainly want to work with you, to do some tweaking, if that is necessary.

Mr. BURGESS. And I thank you for that response. So just in general, with your experience as Chairman of the Federal Trade Commission, you would interpret this draft legislation as strengthening consumer protections across the board?

Mr. LEIBOWITZ. I do. And let me just come back to one question, because it came back in the—came up in the first panel, about the issue dual jurisdiction. And I understand that sometimes the FTC and the FCC work together, and sometimes they can work together very collaboratively.

But just as I believe that the FTC should be the sole Federal enforcer of data security, because I think it does a really good job, and it has expertise, and it is concentrated on that for decades, really going back to the Fair Credit Reporting Act passed in the 1970s, you know, I also wouldn't want to see, for example, the FCC go into the business of spectrum auctions, right? That is something that the FCC does really well. It is a terrific agency at that, and, you know, I think you should just let each agency play to its strengths and to its expertise. Shouldn't be any gaps in the legislation, I don't believe there are, but that is the way, I think, to sort of improve the protections that companies have to have, and ultimately improve the lives of consumers.

Mr. BURGESS. Thank you, sir. Ms. Weinman, let me just ask you, you are a former FTC attorney advisor. Tell me what you see is the difference between privacy and security.

Ms. WEINMAN. Thank you for the question. Privacy relates to how an organization uses data, with whom it chooses to disclose that data. Security relates to the underlying security of that infor-

mation, and the access to which would be unauthorized. That, to me, is the key word in distinguishing between privacy and data security.

Mr. BURGESS. And is that difference important for the subcommittee to consider in its drafting of the bill?

Ms. WEINMAN. Absolutely. I think that, in some ways, privacy and data security are often conflated. But I think, with respect to this bill, you do a good job of separating out the two, and focusing on data security. So I think it is something to keep in mind, because there is often conflation, but I think it is important to keep those two concepts distinguished, and I think this bill does a good job of that.

Mr. BURGESS. Mr. Leibowitz, let me come back to you just on that issue of privacy and data security requirements. Do you feel the bill is doing an adequate job in that regard?

Mr. LEIBOWITZ. I do, Mr. Chairman, and, you know, you can look at them as sort of Venn diagrams with a slight overlap. You can look at them as—along the lines of a continuum. But I think you can separate them. I think you do a very good cut in your discussion draft. And you concentrate on what Mr. Welch said, and Mr. Cárdenas, and others had said, is the most—and Ms. Brooks said is the most important information here is the personally identifiable information. It is what the hackers really care about, right? And that is what you need to have the highest level of protection for, data security, and you need to give notification to consumers.

Mr. BURGESS. Very good. My time has expired. I will yield back. I just want to—time for questions is limited, and I do have some questions that I am going to submit, and ask for a written response, Ms. Cable, in particular for you, and some of the issues that happened around the High Tech Act of Massachusetts, but I will do that in writing.

And I will recognize Ms. Schakowsky. Five minutes for questions, please.

Ms. SCHAKOWSKY. Before—because he has a bill on the floor, I am going to yield right now out of order, Mr. Kennedy, for questions.

Mr. KENNEDY. I want to thank the Ranking Member for the generosity, and, Mr. Chairman, thank you for calling the hearing. To all of our witnesses today, thank you for spending the time, thank you for your testimony. I had the pleasure of introducing Ms. Cable this morning from Massachusetts, so thank for being here, ma'am. And I wanted to get your thoughts, as an enforcement lawyer from Massachusetts—we have heard a number of criticisms of the draft bill today, but I would much rather focus on how we can make this bill stronger, or the data security and breach notification aspects a bit better.

So, in your opinion, ma'am, what are some of the most critical data security standards in Massachusetts law that you believe are not represented within the framework of the proposed bill?

Ms. CABLE. Sure, of course, and I will echo what was previously said by the FTC, and I alluded to in my testimony. You know, this is a framework that includes, at the first step, an evaluation and assessment. What personal information does the company have, where is it, how do they use it? What are the reasonably foresee-

able risks to that information, both internal and external? It is the process of taking stock and evaluating what the risks are that is not reflected in this current draft of the bill that I believe is critically necessary. And you can see that reflected in Gramm-Leach-Bliley standards, and I believe the HIPAA security rule as well.

Stemming from that process are, then, the safeguards that need to be put in place. Again, Massachusetts law leaves open, and gives companies some flexibility, what are the specific safeguards. They include things like restricting employee access to information on an—on a business need basis only. It includes simple things you might not even think about, changing passwords when someone leaves the company, for example.

There is—computer security systems need to be paid careful attention to because of the volume of data they can store, and the many points of access to that data. So perimeter security, such as firewalls, anti-virus protection, software patches. The Massachusetts data security regulations are technology neutral. They leave open, and they contemplate changes in technology and improvement in procedures, but they establish a minimum concept of protecting your computer's security network. There are many more, but, you know, I think it is a process-oriented—it requires a company to take an introspective look at itself and its information, and it is an iterative, evolving process, and I think that is what is important about it.

Mr. KENNEDY. So, given that, Ms. Cable, do you think that should be—or that framework should be a national benchmark, or what additional requirements do you think you could suggest to further enhance the protection of consumers' data?

Ms. CABLE. Well, I think it was suggested in the first panel, and it is the concept of FTC rulemaking authority. And I think that is something—

Mr. KENNEDY. Um-hum.

Ms. CABLE [continuing]. That our office would support a closer look at.

Mr. KENNEDY. And maybe that is the answer to this next question, but how can we ensure that the data security standard is responsive to rapidly evolving technologies and increasingly sophisticated cyberattacks?

Ms. CABLE. I think, you know, giving the FTC the authority and flexibility to, you know, enact regulations that are sufficiently flexible and responsive is one way to do it. And, you know, I haven't heard anyone espouse the opposite of this proposition, which is these need to be neutral, they need to be flexible. There is a way to do that. There are established frameworks in Federal law that do that.

Mr. KENNEDY. So if I—just got about a minute left, and a discussion that has come up over this legislation a couple of times now is over preemption. And so, in your mind, and as a practitioner, can you give us some suggestions on—does it have to be all or nothing, or are there some ways we can preempt some things, like the content of the notice, for example, but not others, to allow for that flexibility?

Ms. CABLE. Absolutely, yes. Thank you for the question. I think preemption absolutely does not need to be an all or nothing ap-

proach. We have heard the patchwork 47 or 51 different data notice regimes, approximately 12 data security standards. What I hear more, regarding a compliance burden, is with responding to a breach, versus how do you prevent a breach in the first instance.

I think there is some work that might be done in limiting the scope of the preemption to address the specific burdens that are being articulated, and enable a rapid response to a breach. But I think the States are innovative in the field of data security, I think they are nimble. You know, our view is the preemption is just simply too broad.

Mr. KENNEDY. I have only got about 10 seconds left. I might submit in writing a question about the—any concerns over the enforcement mechanisms, or the limits on the civil penalties for your consideration.

Ms. CABLE. Of course.

Mr. KENNEDY. Thank you for coming here.

Ms. CABLE. Happy to answer.

Mr. LEIBOWITZ. And if I could just add point to respond to your question? I mean, these are—

Mr. KENNEDY. Yes.

Mr. LEIBOWITZ. It is on my time, or—

Mr. KENNEDY. It is not.

Mr. LEIBOWITZ [continuing]. On your time?

Mr. KENNEDY. It is up to the chairman.

Mr. LEIBOWITZ. If the chairman—

Mr. BURGESS. Gentleman may respond.

Mr. LEIBOWITZ [continuing]. Unanimous consent? Thank you. Again, you raise very good questions about how to think through the next iteration—

Mr. KENNEDY. Um-hum.

Mr. LEIBOWITZ [continuing]. And, obviously, we want to work with you to—

Mr. KENNEDY. Um-hum.

Mr. LEIBOWITZ [continuing]. Do that.

Mr. KENNEDY. OK. Thank you. I appreciate it.

Mr. BURGESS. Chair thanks the gentleman, gentleman yields back. Chair recognize the gentelady from Tennessee, Ms. Blackburn. Five minutes for questions, please.

Mrs. BLACKBURN. Thank you all, and I appreciate the conversation, and—that you would be here and weigh in on the discussion draft. Mr. Leibowitz, I have to say, it looks normal and natural to see you at that witness table, and we are happy to have you back.

Ms. Weinman, I want to come to you first. We haven't talked a lot about the third party notice obligations, so I would like to have you walk through what you see as the strengths and weaknesses of the third party notice obligations.

Ms. WEINMAN. Thank you for the question. I will begin by setting the stage with some defined terms. So the covered entity is generally the entity that has the relationship with the customer, or the consumer, use whichever word you are more comfortable with. And then the third party, or another term used in here would be a service provider, is the one that might perform services on behalf of that covered entity, but would also have personal information in

their possession as a result of their B to B relationship with the covered entity, business to business.

So the gap that I pointed out in my oral statement is that it is unclear when the covered entity would be required to provide notice to its customers when the third party suffered a breach. It is very clear when the covered entity would have to provide notice when it itself had been breached, but when the third party had been breached, it is unclear whether the timeline begins when that third party has had the opportunity to determine the scope of its breach, and had taken steps to remedying vulnerabilities, and restored its systems.

Mrs. BLACKBURN. OK. Let me ask you something else. You mentioned the amount of compliance time, with businesses having to comply with all the different State laws. So is there any way that you can quantify what this would save to businesses by having preemption in place, and having a national standard? Have you thought through it in that regard, as—the cost savings to business?

Ms. WEINMAN. I don't have a quantifiable number, in terms of compliance costs. That is not something that I have put together. I can point out, though, in terms of—the compliance costs would be considerable, considering the legal time. The redirection of resources that could be devoted to other critical areas once a data breach occurs is also a question of opportunity cost. If you are spending a lot of time figuring out your notice regime with 51 different frameworks, that is taking time and money away from other areas that you can be focusing on—

Mrs. BLACKBURN. OK.

Ms. WEINMAN [continuing]. Following a data breach.

Mrs. BLACKBURN. Mr. Duncan, I saw you shaking your head. Let me come to you on that, because you mentioned in your testimony that you all have for years called on Congress to do something on breach notification. You also talk about modeling a Federal bill on strong consensus of existing State laws, and, in the context of third party notification, all of the existing State laws require notice from a third party to a covered entity after a breach.

So I want you to talk to me about two things. I want you to reconcile your support for a national standard based on the State laws with your issues regarding the structure of the State laws for the third party. And then also I want you to talk a little bit about cost, and the preemption, and what it would do to—what it would save consumers and businesses in the process.

Mr. DUNCAN. Thank you, Congressman Blackburn. There are three very good questions. In terms of the States, virtually all of the States do have an arrangement by which third parties would report directly to the entity for whom they were providing, say, a service, and that would be the general rule. What has become increasingly clear to a number of State Attorneys General is that trying to provide notice like that in every situation actually will not provide effective notice.

There is an example, for example, in our testimony that talks about the Hartline breach, which was a huge breach. 80 million data points, I believe, realized. And in that case, Hartline did the right thing. It didn't follow the State laws. In fact, it went beyond them, and provided the notice itself directly. Had they done other-

wise, because Hartline was a payment processor for hundreds of retailers, it would have had—told each of them, and each of them would have had to tell all their customers about Hartline’s breach, so consumers would have received hundreds of notices for what was actually one breach.

So there is becoming a realization among the State AGs that we are—really should be focusing on effective notice, rather than this strictured—structured notice that is contained in some of the State laws. So it is an evolution of that. This presents a double problem when we go to the subset that Ms. Weinman just talked about, which was service providers, because in this case, under the draft language, in some circumstances, they would provide no notice at all, and that certainly—it shouldn’t be a situation that someone who knows they have a notice—knows they have a breach can find themselves in a situation in which they say nothing to anyone, not even to law enforcement.

And finally, as to cost, this is a very significant consideration. You must consider that this law is going to apply not just to the largest companies in America. It is going to apply to the first person who has 15 dry cleaner front—shops. How much will he or she have to stay up at night, wondering about whether or not they have met an amorphous data security standard to—going forward? And that imposes tremendous costs on the operation of our businesses.

Mrs. BLACKBURN. Mr. Chairman, my time has expired, and I will yield back, but I would ask Mr. Leibowitz, I can see that he was trying to respond to that, just to submit in writing his response, or someone later can call on him for his response to that question.

Mr. BURGESS. Chair thanks the gentlelady. Gentlelady yields back. Recognize Ms. Schakowsky. Five minutes for questions, please.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. So I haven’t heard anyone, except for Mr. Leibowitz, say that if the bill were to pass as is that consumers would be better protected. I didn’t hear the first panel or the second panel—it seemed to me that lots of people—everyone had suggestions of how the bill could be made better. If I am wrong, would you tell me that? OK. So I—and Mr. Leibowitz also said he is happy to work with us, so I think we have some work to do.

I wanted to ask a question about personal information that has come up several times. And—so when—let me ask Ms. Cable. In terms of personal information, what does your law include? And I want to ask Ms. Moy kind of a more global—other States as well. Go ahead, Ms. Cable.

Ms. CABLE. Thank you for the question. For Massachusetts, the definition of personal information is actually narrower than what is being considered in this bill. It includes name—first name and last name, or first initial and last name, plus one of the following components, Social Security Number, driver’s license number, or other Government-issued ID number, and that is State Government-issued ID number, or a financial account number with or without the security code required to access the account.

Ms. SCHAKOWSKY. So many of us, I think, think that the requirement in the bill is too narrow, that it is just financial harm. And

I would like to get Ms. Moy, if you could answer, what kind of information do you think is missing now that we are taking this important step of looking toward protecting consumers. What do you think ought to be there?

Ms. MOY. Thank you. Thanks so much for this important question. So, as I mentioned in my testimony, there are a number of pieces of information that are covered by other laws. In particular, health information is covered by a lot of States. But I think, you know, we could go back and forth about particular pieces of information that should or should not be included in the definition of personal information here, but the big picture here is really—the bottom line is that there are broad categories of personal information that are currently covered under a number of State laws, and under the——

Ms. SCHAKOWSKY. Well, let me ask you this, then, because I think it would be—help to outline for us. You noted that this bill does not protect the serious harms that a breach of information could cause, so I am wondering if you could draw a picture for us of what some of those serious harms could be.

Ms. MOY. Sure. So, for example, you could imagine that if your email address and password were compromised. So that might not be an account identifier and a password that is necessarily financial in nature, and would fall within the scope of this bill, but if my personal emails were compromised, I would certainly experience some harm. I am sure I would experience not only emotional harm, but perhaps harm to relationships, perhaps harm to reputation. And, you know, and I think that a common sense question here is just, if my email address and account password were compromised, would I want to be notified? And—absolutely. I think that is just some common sense there.

Ms. SCHAKOWSKY. Let me ask you this. Let us say a woman is a victim of domestic violence——

Ms. MOY. Um-hum.

Ms. SCHAKOWSKY [continuing]. But geolocation is not protected. Could she be at risk in some way?

Ms. MOY. Right, thank you. So I think one of the things that I did highlight in my written testimony is that because both of—the definition of personal information, and the harm trigger that is premised on financial harm, there are categories of information, like geolocation information, or like information about call records, that, if compromised, could result in physical harm. So a domestic violence victim, for example, might be concerned not only about her geolocation information, but perhaps about her call records. If she called a hotline for victim assistance, or if she called a lawyer, those are pieces of information that she absolutely would not want to be compromised.

Ms. SCHAKOWSKY. In terms of the role of the FTC having some flexibility in defining what personal information would be, what position have you taken?

Ms. MOY. Right. So I think it is—I think that it is critical that we provide for flexibility in the definition of personal information in one way or another. Whether it is through agency rulemaking, or through State law, it is really important that we be able to adapt a standard to changing technology, and changing threats.

So I mentioned in my testimony the growing trend of States including medical information in their definition of personal information. In fact, two States just this year have passed bills that will include that information in their breach notification later this year, and that is not an arbitrary change. The reason that that is changing is because there is a growing threat of medical identity theft, and it is really important to build in flexibility to account for those changes.

Mr. LEIBOWITZ. And if I could just follow up on Ms. Moy's points very quickly, in support, I think, of most of them. You know, I think geolocation—and your point. I think geolocation is critically important. When we were at the FTC, we expanded geolocation under COPPA to be a condition present. It is something you may want to take a look at.

It is also important to note that the Massachusetts law, which is one of the most progressive laws of the State, has a narrower definition of data security. This is a well-intentioned piece of legislation, and reasonably we can disagree about where to draw the line, but it is broader than 38 States, that don't have it.

And then the other two very quick points I want to make, on the ISP point that you mentioned before, Mr. Duncan, you know, if a service—aware of a data security breach, they must notify the company of the breach, and they have an obligation to reasonably identify any company, to try to reasonably identify.

And then, finally, on rulemaking, obviously, I came from the FTC, I came and testified in support of this legislation, or signed testimony. I would just say, and maybe this is overall for the legislation, this is my belief in it, it always was when I was there, is you just don't want to let the perfect be the enemy of the good here. You want to make sure you move forward for consumers. Reasonable people can disagree about exactly where that is, but getting some things sometimes is better than, you know, not getting everything.

Mr. BURGESS. The Chair thanks the gentleman for his observations. Gentlelady's time has expired. Chair recognizes the gentlelady from Indiana, Ms. Brooks. Five minutes for questions, please.

Mrs. BROOKS. Thank you, Mr. Chairman, and I want to build on what the gentleman from Massachusetts was saying, is that we have to get this right, and—perfect is the enemy of good here. And I have heard—I am not familiar with Massachusetts statute, and, obviously, with there being so many statutes, the problem is that we in Congress, while we have been talking about it for years and years and years, and I applaud all the work that has been done in Congress in the past, we have got to move something forward here, because terrorist organizations, nation-state organizations, they are going to always continue to come up with more ways and new ways to hack and get this information.

And it is becoming, I think, one of our constituents' greatest security concerns, truly, and we have got to get this right. And I don't believe that having 51 different standards is good. We have got to get, you know, we have got to move on this and improve. And I think—my previous question to the director of the FTC, the reasonable security practice, and if we were to adopt, for instance,

Massachusetts, how you have set out, and what I would love to see is the State Attorneys General work with the committee and the members who have put forth this legislation, and let us get this right.

And so, for instance, if the reasonable security practices that you delineate in Massachusetts, those are flexible, but yet they set out the process, would that satisfy you on the reasonable security piece, Ms. Cable?

Ms. CABLE. Yes, thank you for the question, and I agree and appreciate this is a critical issue, and there needs to be action, and I really applaud the subcommittee for taking up this issue, because it is complicated and it is difficult.

I think, you know, I happen to very much like the Massachusetts data security regulations, but, of course, I have to say that.

Mrs. BROOKS. Sure.

Ms. CABLE. I think they are, however, a good framework, a recognized framework, and something that commercial entities are used to seeing. And I think the issue with preemption, what makes it concerning to us, is the standard of data security that is being set. We don't think it is sufficiently defined, and therefore we think, as a result, it may not be sufficiently robust. And so, at least from Massachusetts perspective, this is not better off for our consumers if reasonable security measures and practices result in a downward harmonization across the Nation of a lower standard of security.

And I might add, lower security, logically, I think, will result in an increased incidence of breaches, an increase in notice obligation, and an increase of all of the problems we are discussing today. I really think the data security standard is a critical element. I think the reasonableness standard is maybe a good lode star guidepost, but this—the measures and practices need to be more defined.

Mrs. BROOKS. Mr. Leibowitz, would you like to comment on those remarks?

Mr. LEIBOWITZ. Well, I mean, at 50,000 feet I agree that you don't want to ratchet down, you want to ratchet up the level of data security. I think the fact that 38 States don't have any data security obligations at all is very telling. And, again, as Ms. Cable acknowledged, you know, one of the most progressive pieces of legislation that States have written is the Massachusetts law. On the data security side, it has a narrower definition.

So I think, again, and going back to Mr. Welch's point and Mr. Cárdenas' point, it is like what do people care about when—what hackers care about, they care about the personal identification and the financial information. And what do consumers care about, and at the FTC—and the FTC continues to do great work here, you know, they care about their Social Security Number. They care about their financial information being taken. They care about, you know, economic harm more than anything else. And that is what drives this problem more than anything else. It is not ideological groups. It is, you know, people engaged in fraud and criminal activities that the FTC and the State AGs have been prosecuting, will continue to be able to do in the bill.

Mrs. BROOKS. Thank you. And one completely different issue, Ms. Weinman, you talked about the providers must restore their system, that entities should restore their system before notification.

Can you explain why that would be necessary when it does seem that speed in getting out notifications—although we know that often those who are breaching and hacking can sit on this information for years, they don't often use it immediately. But why do you propose that an entity needs to have the time to restore its system, as you have said, before notification?

Ms. WEINMAN. As currently drafted, the bill does allow that restoration of system for a covered entity, and I think it is critical that that be the case because if an entity provides notification, it is essentially making public that its system has been compromised, and it could render itself further vulnerable to additional attacks by those same hackers, or other hackers. So I thank, and applaud, the subcommittee for recognizing that point in time when notification should begin should be at a time when the system has been restored.

Mrs. BROOKS. Thank you. I yield back.

Mr. BURGESS. The Chair thanks the gentlelady, and Chair recognizes the gentleman from Vermont, Mr. Welch for 5 minutes for questions.

Mr. WELCH. Thank you very much, sir. I want to take up a bit from where my colleague, Ms. Brooks, was with the Attorney General's Office from Massachusetts. First of all, thank you for your testimony. Second, thanks for the good work that Massachusetts does. Third, we are pretty proud of our Attorney General and consumer protection in Vermont. They have a standard and an—they have a solid standard, and an aggressive consumer protection division, like you do, and they have made some of the same arguments to me about this bill that you just made, so message received.

But I just wanted to go through a few things. Number one, the bill does use this term reasonableness, and I think there has been a debate, even—not—on all sides, including among consumer activists, whether something that is flexible has the potential to meet the challenges as they emerge, as opposed to—what I heard in your testimony is a more detailed set of guidelines that is—according to your testimony is working for you.

But I guess I am just looking for some acknowledgment that there is a legitimate argument to approach it in a prescriptive way, or in a general way that gives a little more flexibility to the enforcer, in this case Massachusetts. Would you agree with that?

Ms. CABLE. Yes, thank you for your question, and I would reiterate I work closely with colleagues from the Vermont Attorney General's Office. It is a fantastic office, and I enjoy working with them. I think the issue of data security standards, and whether they are flexible—

Mr. WELCH. Right.

Ms. CABLE [continuing]. Flexible or prescriptive, I think you can have standards that articulate components of what a data security system framework should look like, but an awful lot of flexibility with how you meet those standards, and I—

Mr. WELCH. Well, right, and that is where it is genuinely difficult. Because, you know, if Ms. Brooks was able to get all the Attorney Generals to come up with what was the best approach, that might be persuasive to all of us, because there are Republican and Democratic Attorney Generals out there.

A second thing that I wanted to talk about is this question of an obligation on the part of the companies. There is an enormous incentive for thieves, criminals, to try to hack our information. They get our money. There is an enormous incentive—I am looking for all you—your reaction on this—for companies to have their computer systems be as safe as possible, because they are victims too in this case. I mean, look what happened at Target. People lose their jobs. It is brutal on the bottom line for these companies. So I see that as a practical reality that we can take advantage of. I mean, is that consistent with you, as an enforcer?

Ms. CABLE. I would absolutely agree, and I would note, you know, much of my effort is not spent trying to find gotcha moments and——

Mr. WELCH. Right.

Ms. CABLE [continuing]. Enforcing. We have received notice of over 8,600——

Mr. WELCH. Yes.

Ms. CABLE [continuing]. Breaches, and I think, we ran the numbers, we have had 13 actions.

Mr. WELCH. But you would be in agreement——

Ms. CABLE. I would, and I would——

Mr. WELCH. Yes.

Ms. CABLE. Most of my time is spent——

Mr. WELCH. I don't have much time, so let me get a——

Ms. CABLE. Of course. I apologize.

Mr. WELCH [continuing]. Few more. You have been very helpful. The other thing Mr. Duncan was talking about, effective notice, and this goes back, again, to kind of practicality. If I get these bank notices when I do this mortgage refinancing, it literally gives me a headache, and I get less information. All I need to know are three things, what is my rate—what is my interest rate, when is the payment due, and what is the penalty if I don't meet the time? That is all I need to know. And—so this effective notice issue, I think, is something that, on a practical level, all of us want to take into account.

So let me go, Ms. Moy, to you. I want to, first of all, thank you and your organization for the great work you have done, and also for being available to try to answer my questions.

Ms. MOY. Thank you.

Mr. WELCH. You had mentioned something that every single one of us would be really concerned about, if there was any way that we were passing legislation that was going to make a woman of domestic violence more vulnerable. All of us would be against that, OK? So I don't see in this legislation how that is happening, but if, in your view, it is, I would really welcome a chapter and verse specification as to what we would have to do to make sure that didn't happen. And I think we would all want to be on board on that. So could you help us with that——

Ms. MOY. Thank you, I appreciate that question, and I have appreciated working with your office as well. So I think, you know, this question mostly gets to what standard is set for the harm trigger, right? I mean, because there are certain types of information, or certain situations where information may be compromised or accessed in an unauthorized manner, and you could look at that

situation and say, this information really couldn't be used for financial harm, or we think it is unlikely that that is the—that was the motivation of the person who accessed that information.

Mr. WELCH. OK. My time is running up, so I——

Ms. MOY. Yes.

Mr. WELCH [continuing]. Apologize for interrupting, but if——

Ms. MOY. Um-hum.

Mr. WELCH [continuing]. You sent us a memo on that, and——

Ms. MOY. Absolutely.

Mr. WELCH [continuing]. Attorney Cable, if you sent us some specifics, that would be helpful to the committee, because I know Ms. Schakowsky was very interested in a lot of the points you made, as well as all of us, I think.

Ms. MOY. Absolutely.

Mr. WELCH. Thank you.

Ms. MOY. Thank you.

Mr. WELCH. I yield back.

Mr. BURGESS. Chair thanks the gentleman. Chair recognizes the vice chair of the subcommittee, Mr. Lance. Five minutes for questions, please.

Mr. LANCE. Thank you very much, Mr. Chairman.

Mr. Leibowitz, in your opinion, what benefit have class actions brought to consumers after a data breach?

Mr. LEIBOWITZ. Well, let me start by saying, I think class actions have an enormous value in a lot of areas. Civil rights areas, others as well. In this area, I don't think that class actions have much benefit, except for the lawyers who bring them. And what they also do is they incentivize, or the create incentives, I think, for companies to emphasize legal protections, rather than actual reasonable data security.

And I will just make sort of one other point, which goes back to the FTC, which is, if the FTC brings a case, and it gets compensation for consumers, all that compensation goes back to the consumers. They—\$200 million to 400,000 people who were victims of mortgage service fraud by Countrywide, and that is one other benefit. But I also believe that, you know, class actions can be vitally important, as I am sure you do, in some areas.

Mr. LANCE. In other words, your point is that when the FTC does it, the—FTC personnel are in the public sector, and the full benefit goes to those——

Mr. LEIBOWITZ. The entire——

Mr. LANCE [continuing]. Who have been harmed?

Mr. LEIBOWITZ. Yes.

Mr. LANCE. It is an indication why we should be supportive of our Federal workforce——

Mr. LEIBOWITZ. And——

Mr. LANCE [continuing]. And for colleagues who serve in Federal service. Would others like to comment on that? Attorney General Cable?

Ms. CABLE. If I may?

Mr. LANCE. Certainly.

Ms. CABLE. Thank you, Congressman.

Mr. LANCE. Certainly.

Ms. CABLE. I would just note—consumer restitution is a critical tool that we have in our toolbox under our Consumer Protection Act. We use it—we like to use it. If we can get the money, we distribute it. I noted under this version of this bill, it does not expressly allow us to seek consumer restitution, and it also denies the consumer a private right of action. We think that is a bit of an oversight in the event a consumer is actively harmed here. State AGs under this bill would not be able to seek consumer restitution, under one interpretation.

Mr. LANCE. Thank you, Attorney General. Mr. Leibowitz, do you wish to comment further or not? No? Thank you.

Mr. LEIBOWITZ. No, sir.

Mr. LANCE. Ms. Weinman, do you have a concern about State common law claims adding additional security or notification requirements for companies if a Federal law is enacted?

Ms. WEINMAN. I think that this bill strikes a useful balance in pre-empting the current State data security requirements and the breach notification, so I think this bill strikes a good balance in that area.

Mr. LANCE. And you believe that because the country would move forward uniformly, and this would be something that would be on the books for the entire Nation?

Ms. WEINMAN. Yes, and it would streamline the notification process across the board, across the 51 regimes for which I have, you know, a 19 page chart. So I think that would definitely be useful.

Mr. LANCE. Yes. Thank you. Mr. Chairman, I yield back the balance of my time.

Mr. BURGESS. Chair thanks the gentleman. Chair recognizes the gentleman from New Jersey, Mr. Pallone. Five minutes for questions, please.

Mr. PALLONE. Thank you, and I have been to, like, three different meetings since I was last here, so hopefully I will be understandable here. Under current law the FTC does not have enforcement authority over common carriers, including telecommunications, cable, and satellite services, and the discussion draft lifts the common carrier exception to allow the FTC to bring enforcement actions for violations of the provisions of this bill.

And I wanted to ask each member of the panel, and I am just looking for a yes or no because I have a whole series of things here, if you could just say yes or no, assuming the draft did not include preemption of the Communications Act in Section 6C, do you support lifting the common carrier exceptions in the context of data security and breach notifications, yes or no? We will start to the left.

Mr. LEIBOWITZ. Yes.

Mr. PALLONE. Ms. Cable?

Ms. CABLE. I apologize, I think I am out of my expertise, so—

Mr. PALLONE. You have no response?

Ms. CABLE. I have no response.

Mr. PALLONE. All right. Mr. Duncan?

Mr. DUNCAN. We don't have a preference as to which agency covers it.

Mr. PALLONE. That is—

Mr. DUNCAN. The only requirement is that everyone be covered.

Mr. PALLONE. OK. Ms. Moy, yes, no?

Ms. MOY. If it did not eliminate provisions of the Communications Act, yes.

Mr. PALLONE. OK. And our last——

Ms. WEINMAN. I will give a similar response to Mr. Duncan, that it is not an issue that would implicate ITI members, so——

Mr. PALLONE. All right.

Ms. WEINMAN [continuing]. I am not expressing a preference one way or the other.

Mr. PALLONE. All right. Now I just want to ask my next two questions of Ms. Moy, because I may not have a lot of time. Lifting the common—I have two. First, lifting the common carrier exception without nullifying the data security and breach notification provisions of the Communications Act would mean that there are two cops on the beat, so to speak, so what are the benefits to joint jurisdiction among the FCC and the FTC? To Ms. Moy only.

Ms. MOY. Thank you, thank you so much. So I think one of the major benefits is that the two agencies have different strengths, and they could work together to use their strengths to complement each other and ensure the best protection for consumers. For example, the FCC is primarily a rulemaking agency that uses its authority to set standards prospectively, and the FTC is primarily an enforcement authority. It would be really nice if they could work together to establish the standards in the first place, and then enforce them in the second place.

I think also the FCC has a lot of very important expertise in this area, working with telecommunications networks, and other communications networks, and just—and the focus on privacy is a little bit different. The focus on privacy at the FCC is more about the reliability of the networks, and the fact that consumers have no choice but to share information with these very important networks in their lives, whereas the focus of the FTC on privacy is a little bit more about what is fair with respect to consumers. And, again, it would just be really nice if those agencies could work together in that area to use their expertise, or their respective expertise, in a complementary manner.

Mr. PALLONE. And then I have a second one to you only, and if I have time, we are going to go to the others. Do you think there are any drawbacks to having FTC and FCC enforcement? Are you concerned about consumers being confused by having two enforcing agencies?

Ms. MOY. I am not concerned about that. I think that where we have seen agencies work together in the past, I don't think that there really is confusion for consumers. For example—I am sorry, I am blanking, but the FTC and the FCC have worked together on the, for example, Do Not Call, of telecommunications customers. And I really don't think that there is any risk of confusion for consumers of having those agencies work together.

Mr. PALLONE. All right, one more question. I will start with you, and then—we have time, we will go to the others. Do you have any suggestions for how legislation can ensure that companies are not burdened by duplicative enforcement?

Ms. MOY. I am sorry, that companies are not burdened by——

Mr. PALLONE. By duplicative enforcement. Any suggestions for how legislation could ensure that companies are not burdened by duplicative enforcement?

Ms. MOY. Well, the premise of the question is that duplicative enforcement is necessarily more burdensome for companies, and I don't think that that is necessarily the case. You know, as I said, the FCC and the FTC can work together to formulate standards and enforce them in a uniform way. And I think that they would have an incentive to do that, so as to maximize the efficiency of their resources toward that goal. And I think that that incentive would sync up quite nicely with the incentive of having the two agencies work in step with each other, so as not to seem like two totally separate regimes.

Mr. PALLONE. All right, thanks. I think I have run out of time, Mr. Chair.

Mr. DUNCAN. If I—

Mr. PALLONE. Thank you.

Mr. DUNCAN. If I might just mention, on that point, under the structure of the bill, both the FTC and the State AGs would have enforcement authority, and that is an option that works, at least in that context. From our perspective, as long as everyone has the same obligations, and duties, and responsibilities, then it is less of an issue.

Mr. LEIBOWITZ. Yes. And the only thing I would add is that there sort of an evolving consensus that what you really want, Mr. Pallone, is a flexible enforcement standard that is strong with enforcement. And you also want to treat the same information the same way, not under different regimes. So, you know, Google can collect information, Verizon can collect information, Comcast can collect information. A variety of other companies can.

And, for the most part, I think where this bill wants to go is in a data breach context. And in the data security context, more importantly, treat them equally.

Mr. BURGESS. Chair thanks the gentleman. Gentleman's time has expired. Chair recognizes Mr. McNerney. Five minutes for your questions, please.

Mr. MCNERNEY. Well, I want to thank the chairman and the ranking member for allowing me to participate in this hearing, even though I am not a member of the subcommittee. I appreciate that. And I want to say I appreciate the efforts of my colleagues, Mr. Welch, Mr. Burgess, and Mrs. Blackburn for crafting this bill. It is clearly needed. And it may not be perfect yet, but it can be improved, and it is much better to start from the draft than to start over—than to over to start over. So I have a couple of questions here.

Ms. Weinman, you mentioned that the civil penalties for breach of notification are excessive for a company that is a victim of a criminal act. Do you think it would be OK to lower the penalties, or to have some flexibility? And if you think flexibility is the way to go, how can you do that in this kind of a bill?

Ms. WEINMAN. I think lowering would be a good step, and I think there is flexibility built into the assessment of civil penalties within the bill, but I think lower the maximum penalties would make sense in the context of the fact that companies themselves are the

victims of criminal hackers. So there is some discretion with regard to civil penalties within the bill, however I do think the maximum amounts set out in there should be lower. And I note that the current figures in there are, in fact, five times higher than what we have previously seen in other proposals, so I just make a note of that.

Mr. MCNERNEY. Well, I mean, you could consider some breaches to be gross negligence, and deserving of significant penalties, so—

Ms. WEINMAN. Well, that flexibility is built into the language, but I do think that the ceiling could be lower in the draft.

Mr. MCNERNEY. Thank you. Ms. Moy, you know, preemption is a very tricky issue. We want States to have flexibility, but you mention that there ought to be a floor. But how could you create legislation that had a floor, but allowed States like Massachusetts flexibility to go, you know, more stringent, if they wanted?

Ms. MOY. Thank you for the question, and thank you. I do recognize that it is very difficult to craft the appropriate standard here, and thank you for taking up this difficult issue. I, you know, I think that you could set a standard that says, this is the minimum standard, and that State laws will not be preempted to the extent that they create additional standards above that, or beyond that.

But, you know, but also, as I have said in the written testimony, and as I mentioned earlier, we are not necessarily opposed to the idea of preemptive legislation, but I do think that it is important, if we are going to do that, to ensure that the new Federal standard, the new uniform Federal standard, is better for consumers than the current draft. I just—I think it is really important to strike the proper balance between preemption and protections for consumers, and this just doesn't quite get us there.

Mr. MCNERNEY. Now, you mentioned that you felt that the draft would lower consumer protections over a wide range of consumer protections. Could the bill be strengthened to include those current protections?

Ms. MOY. I believe that it could be, and I think—I would be very happy to work with the subcommittee to figure out ways that we could get there.

Mr. DUNCAN. Congressman—

Mr. MCNERNEY. Thank you.

Mr. DUNCAN [continuing]. One of the reasons that we are here today is because there are already 51 conflicting laws out there. If Congress doesn't simplify the system to some extent, then we will simply have 52 laws out there, and that is not moving us forward.

Mr. MCNERNEY. Thank you. Well, Mr. Duncan, you mentioned that—the importance of enacting laws that holds accountable all entities that handle personal information. Can you discuss how you would improve the draft legislation to modify the covered entities?

Mr. DUNCAN. Certainly. We would expect that a good law would require that every covered entity have the same obligation, that third parties—for example, the way the bill is written now, some entities do not even have a duty to determine—to examine and determine whether or not they can find information out about a breach. There has got to be the same level requirement all the way across the board.

Congresswoman Schakowsky asked earlier whether or not we could support this legislation. I would say this draft is a major improvement over what we have seen before, but if we could have equal applicability across all entities, and fix some of the issues with the FTC, we could support this.

Mr. MCNERNEY. Thank you—a lot of good information has come out that might help improve the bill, so, Mr. Chairman, I yield back. Thank you again.

Mr. BURGESS. Chair thanks the gentleman. Gentleman does yield back. The Chair recognizes Mr. Pallone of New Jersey for a unanimous consent request.

Mr. PALLONE. Thank you, Mr. Chairman. I ask unanimous consent to submit for the record a letter from 12 consumer groups to yourself and Ms. Schakowsky.

Mr. BURGESS. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. PALLONE. I guess we have another one, too, Mr. Chairman, from the Consumers Union, in addition to the one from everyone else.

Mr. BURGESS. The Chair thanks the gentleman. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. BURGESS. Seeing that there are no further members seeking to ask questions, I do want to thank all of our witnesses. I know this has been a long hearing, but I thank you for participation today.

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 Credit Union National Association; a letter on behalf of the Marketing Research Association; a letter on behalf of the National Association of Federal Credit Unions; a letter on behalf of the Online Trust Alliance; a letter on behalf of the Consumers Union; statement on behalf of the National Association of Convenience Stores; a letter on behalf of the American Bankers Association, The Clearing House, Consumer Bankers Association, Credit Union National Association, Financial Services Roundtable, Independent Community Bankers of America, and the National Association of Federal Credit Unions; and the response of the Secret Service to questions submitted for the record at our previous subcommittee data breach hearing on January 27, 2015.

[The information appears at the conclusion of the hearing.]

Mr. BURGESS. Pursuant to committee rules, I remind members they have 10 business days to submit additional questions for the record, and I ask witnesses to submit their response within 10 business days upon receipt of the questions. I thank everyone for their participation this morning. This subcommittee hearing is adjourned.

[Whereupon, at 1:16 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

March 18, 2015

The Honorable Michael C. Burgess & Jan Schakowsky
 Chairman & Ranking Member
 Subcommittee on Commerce, Manufacturing & Trade
 Energy & Commerce Committee, House of Representatives
 Washington, DC

RE: Data Security and Breach Notification Act of 2015

Dear Chairman Burgess and Ranking Member Schakowsky:

We are twelve organizations representing the public interest in the areas of privacy and consumer policy. We write to express our strong opposition to the draft Data Security and Breach Notification Act of 2015. As currently written, the bill severely undercuts communications data breach protections upon which millions of Americans rely, by superseding key parts of the Telecommunications Act of 1996 as implemented in rules promulgated by the Federal Communications Commission.

Communications record data is among the most private information we have “because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person’s life.”¹ A Pew survey from just five months ago found that 67% of Americans expected that telephone calls were somewhat or very secure.² And a breach of that security could cause emotional or even physical harm:

- Telephone records can reveal damaging and even potentially threatening information. Domestic violence victims who contact support hotlines would be in danger of abuse; political candidates’ donors could be revealed; calls to suicide hotlines or emotional support centers would be discouraged.³
- Laws protecting our most confidential data, such as health and financial records, depend on communications security.⁴ Without strong security for communications, that sensitive information could be left out to dry.
- Communications data underlies the mass surveillance programs that many have opposed and decried. Weakening protections on that data will only open the door to further abuse of that data for surveillance purposes.

For decades, the Communications Act has protected this sensitive information about communications network usage. Sections 201 and 222 of that Act ensure that providers implement strong protections for a wide range of data, termed “customer proprietary network information” or “CPNI.”⁵ The FCC uses both rulemakings and enforcement actions to keep those protections in step with modern technological developments.

¹ *Smith v. Maryland*, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

² Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (2014), available at <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

³ See Timothy B. Lee, *Here’s How Phone Metadata Can Reveal Your Affairs, Abortions and Other Secrets*, Wash. Post, Aug. 27, 2013.

⁴ See 42 U.S.C. § 17932 (health care data); 15 U.S.C. § 6801 (financial records).

⁵ 47 U.S.C. § 222(h)(1).

The Honorable Michael C. Burgess & Jan Schakowsky

March 18, 2015

Page 2

But section 6(c) of the proposed Data Security and Breach Notification Act of 2015 would replace many of those key protections with weaker standards:

- It would require companies to notify consumers of a data breach only if financial harm—not emotional or physical—were likely to occur as a result of the breach. As explained above, breach of communications data can result in numerous kinds of emotional or physical harms, harms avoided by the CPNI statutes and regulations⁶ but not by the proposed bill.
- It allows numerous communications data breaches to go unnoticed and unremedied. While the FCC requires every breach that occurs to be reported,⁷ the bill only requires notification to the Federal Trade Commission of data breaches where over 10,000 records were lost.⁸ Thus, many smaller data breaches may be under-reported, under-investigated, and under-deterred.
- It eliminates the rulemaking authority that has allowed for the CPNI privacy protections to keep in step with the times. The FCC can implement new rules, such as its 2007 rules responding to “pretexting.”⁹ But the FTC, to whom data breach oversight would be transferred, has no such ability, and thus will be shackled to preventing data breaches of the future using the law of the past.

This excoriation of communications data breach protection could not come at a worse time, right on the heels of the FCC’s historic open Internet order. Millions of Americans called for the FCC to reclassify broadband Internet as a telecommunications service under Title II of the Communications Act. The FCC listened and reclassified broadband to protect the open Internet.¹⁰

Following reclassification, Sections 201 and 222 of the Communications Act will now apply to broadband providers, vesting the FCC with strong authority to further protect consumers’ information in the broadband sphere.¹¹ As the order explains, “consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth.”¹² As the phone networks transition to Internet-based systems, that Internet privacy becomes only more important, to ensure that the privacy expectations of those 67% of Americans are maintained. And so FCC Chairman Tom Wheeler stated that, in the wake of the reclassification order, consumer privacy will be a top issue for the Commission. “Privacy is not a secondary activity here,” he said; “Privacy is an important issue to us.”¹³

⁶ See 47 C.F.R. §§ 64.2010–2011.

⁷ See 47 C.F.R. § 64.2009(e).

⁸ See Data Security and Breach Notification Act of 2015, sec. 3(a)(3).

⁹ See Implementation of the Telecommunications Act of 1996, 67 Fed. Reg. 59205 (Sept. 20, 2002).

¹⁰ See Report & Order on Remand, Declaratory Ruling, and Order, FCC GN Docket No. 14-28 (Mar. 12, 2015), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.

¹¹ *Id.* ¶ 462.

¹² *Id.* ¶ 54.

¹³ Adam Sneed, *Privacy is the Star at “Tech Prom,”* Politico Morning Tech, Mar. 11, 2015, available at <http://www.politico.com/morningtech/0315/morningtech17426.html>.

The Honorable Michael C. Burgess & Jan Schakowsky

March 18, 2015

Page 3

To eliminate those data breach protections that consumers currently enjoy under the Communications Act, to take authority from a commission with decades of experience regulating use of personal information by communications providers, to cut back on the FCC's ability to protect consumers when the FCC has prominently expressed its commitment to protecting them—these would not merely be a mistake. These would be an affront to the American people's expectations for privacy and for their communications services.

We certainly look forward to an ongoing discussion with the Subcommittee and Congress on how to strongly protect consumer privacy and data security.¹⁴ But a bill that cuts back on the privacy guaranteed by the Communications Act with no sufficiently corresponding benefit is not acceptable to us. We cannot support this bill, and encourage you and the Subcommittee to oppose it.

Sincerely,

Public Knowledge
Center for Media Justice
Common Cause
Consumer Federation of America
Media Action Grassroots Network
Consumer Action
Consumer Watchdog
Center for Digital Democracy
U.S. PIRG
Privacy Rights Clearinghouse
Future of Music Coalition
Free Press Action Fund

Cc: Members of the Subcommittee

¹⁴ Cf., e.g., Letter to Senate Commerce Committee on the Personal Data Notification and Protection Act (Feb. 4, 2015), available at http://www.consumerfed.org/pdfs/150205_Senate-Commerce_Letter_data-breach-hearing.pdf.

ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

March 18, 2015

The Honorable Michael C. Burgess, M.D.
 2336 Rayburn House Office Building
 Washington, D.C. 20515

The Honorable Jan Schakowsky
 2367 Rayburn House Office Building
 Washington, D.C. 20515

Dear Representatives Burgess and Schakowsky:

Consumers Union, the advocacy arm of Consumer Reports, writes you regarding today's Subcommittee on Commerce, Manufacturing, and Trade hearing on a discussion draft of the Data Security and Breach Notification Act of 2015. While we appreciate the Subcommittee's attention on commercial data breaches, we have several major concerns with the draft legislation.

First, in preempting state-level breach notification laws, the draft replaces generally broader, stronger notification standards with generally narrower, weaker ones. Several state breach notification laws, such as those in California, Florida, and Texas, include types of personal information not covered by this draft, and most states do not require a risk of financial harm as a prerequisite for notification. These states rightly recognize that consumers can be harmed by compromises affecting many types of data, including health and medical information.

Second, the draft's information security provision does not improve the level of protection of consumer data, and for some states, significantly reduces it. The draft's "reasonable security measures and practices" standard appears roughly equivalent to what the Federal Trade Commission (FTC) enforces under its existing authority; however, the actual protections afforded consumers by this standard are not articulated, and are likely to be determined by the courts. State laws protecting consumer data in more specific ways, like in Massachusetts and Nevada, would be invalidated, and no state could pass such a law later.

Lastly, the draft jeopardizes protections for consumer data held by telecommunications, cable, and satellite providers. Currently, for example, data related to telephone calls or viewing history are subject to strong data security and breach notification standards overseen by the Federal Communications Commission (FCC). Under this draft, such information would be subject to lesser standards under this bill enforced after-the-fact by FTC, or no standards at all.

The discussion draft before the Subcommittee does not represent a step forward for consumers, and our organization could not support it as currently written. We look forward to working with the Subcommittee to address the issues we have raised.

Sincerely,

Ellen Bloom
 Senior Director, Federal Policy and
 Washington Office

William C. Wallace
 Policy Analyst



Jim Nussle
President & CEO

601 Pennsylvania Ave., NW
South Building, Suite 600
Washington D.C. 20004-2601

Phone: 202-508-6745
Fax: 202-638-7734
jnussle@cuna.coop

March 17, 2015

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

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

Dear Chairman Burgess and Ranking Member Schakowsky:

On behalf of the Credit Union National Association, I am writing to thank you for holding a hearing entitled "Discussion Draft of H.R. _____, Data security and Breach Notification Act of 2015". CUNA is the largest credit union advocacy organization in the United States, representing nearly 90% of America's 6,300 state and federally chartered credit unions and their 102 million members.

Credit unions are subject to high data protection standards under the *Gramm-Leach-Bliley Act*, and they take their responsibility to protect their members' data seriously. Unfortunately, there is a weak link in the payments system that leaves consumers' financial data vulnerable to theft by domestic and international wrongdoers. The weak link is the absence of Federal data security standards for the merchants that accept payment cards.

There have been several very high profile merchant data breaches in the last few years, notably the breaches at Target in 2013 and Home Depot in 2014. Millions of credit union members were affected by these two breaches, which ultimately cost credit unions – and by extension their members – nearly \$100 million. Despite the recovery efforts of payment card networks, no credit union has received a dime from the merchants whose security failure allowed the breach. Credit unions and their members are left on the hook.

These two breaches made headlines, but merchant data breach is a chronic issue. The endless string of breaches demonstrates clearly that those who accept payment cards need to be subject to the same Federal data standards as those who issue the cards.

It is important to recognize that the costs of a merchant data breach scenario on a small financial institution will be relatively greater than the costs of the same breach on large financial institutions. For example, credit unions do not enjoy the economies of scale that national megabanks do. Therefore, the cost of everything, from replacing a debit card to monitoring suspicious activities, is greater.

The Honorable Michael C. Burgess
 The Honorable Jan Schakowsky
 March 16, 2015
 Page Two

Credit unions join with our colleagues in the banking industry to call on Congress to enact meaningful data security legislation that incorporates the following principles:

- 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.
- Banks and credit unions are already subject to robust data protection and notification standards. These *Gramm-Leach-Bliley Act* requirements must be recognized.
- Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification standards.
- 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 breach, including the entity at which the breach occurred.
- 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.

There are a number of Congressional committees exploring remedies to merchant data breaches. Given the very direct and detrimental impact these breaches have on credit unions and banks, we have asked the House Financial Services Committee to take a leadership role in this effort. We understand and appreciate that the staff of the Energy and Commerce Committee and the staff of the House Financial Services Committee have recently discussed these matters together.

In addition to incorporating the principles outlined above into the legislation you are considering, we would like to bring to your attention a technical issue that we hope you will correct. We appreciate that you have exempted from the definition of covered entity certain financial institutions as defined under Section 5(a)(2) of the Federal Trade Commission Act. While this definition would exclude from the definition of covered entity all federally chartered credit unions, it does not exclude state chartered credit unions. That

The Honorable Michael C. Burgess
The Honorable Jan Schakowsky
March 16, 2015
Page Three

is why we suggest adding to Section 5(4)(B) on page 19 the following: "(iii) a depository institution as defined in section 19(b)(1)(A) of the Federal Reserve Act." This ensures that state chartered credit unions are included in the exemption of covered entities.

On behalf of America's credit unions and their 102 million members, thank you for considering our views on this very important topic for America's consumers, which we are proud to serve as their financial institutions – we must all share responsibility in protecting consumer data.

Sincerely,

A black rectangular redaction box covering the signature of Jim Nussle.

Jim Nussle
President & CEO



March 16, 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: Endorsement of the Data Security and Breach Notification Act of 2015

Dear Chairman Burgess and Ranking Member Schakowsky,

On behalf of the Marketing Research Association (MRA),¹ I write to share our endorsement of the draft legislation from Reps. Marsha Blackburn (R-TN) and Peter Welch (D-VT), "The Data Security and Breach Notification Act of 2015." This bipartisan bill will set a national standard to help protect consumers' sensitive information from the ravages of identity theft, fraud, and other criminal abuse, without impeding the essential work of the survey, opinion and marketing research profession.

MRA is happy to endorse the Act because it:

- **Sets a national standard.** Federal preemption of the mishmash of state data security laws is essential.
- **Concise defines personally identifiable information (PII).** This legislation carefully limits the data covered to that which is most likely to lead to criminal abuse in the wrong hands, and exempts encrypted or otherwise deidentified or unreadable data. Unlike the President's draft bill, which included broad account access information (presenting potential privacy concerns, not necessarily security ones), the Blackburn/Welch limits that to identifiers and passwords "required for an individual to obtain money, or purchase goods, services, or any other thing of value."
- **Explicitly establishes the FTC's authority over data security, and provides regulatory flexibility.** The FTC's authority to regulate and enforce data security, which has been questioned in court by Wyndham Hotels and LabMD, is explicitly put into law with this Act. The Act also avoids setting specific requirements for data security programs, since the FTC will need flexibility. However, the Blackburn/Welch bill does well in NOT giving the FTC extraordinary APA rulemaking authority – the agency's existing authority is sufficient. The gravest mistake would have been to follow the President's lead and allow the FTC such extraordinary powers to alter the definition of PII. The agency would undoubtedly expand the definition radically, since FTC Commissioner Ramirez² and others at the agency have said that they consider almost any data to ultimately be personally identifiable. The FTC will still be able to modify the definition using its regular Magnuson-Moss rule-making authority, and that should be sufficient.
- **Requires consumer notification within a reasonable (and not arbitrary) timeframe.** The Act demands that businesses notify consumers about a breach "as expeditiously as possible and without unreasonable delay," but specifically no more than 30 days after having "taken the necessary measures to determine the scope of the breach of security and restore the reasonable integrity, security, and confidentiality of the data system."

While a few specifics still need to be ironed out, especially the full extent of preemption of state laws, the Act will bring certainty for American businesses and companies, including survey, opinion and marketing researchers, whose livelihood depends on the legitimate and accurate collection and analysis of information provided by consumers. MRA looks forward to the Subcommittee's hearing on March 18 and working with you to shuttle this bipartisan solution into law.

Sincerely,

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

¹ 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.

² 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."



3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org

National Association of Federal Credit Unions | www.nafcu.org

March 16, 2015

The Honorable Fred Upton
Chairman
House Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

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

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

Re: Discussion Draft of the *Data Security and Breach Notification Act of 2015*

Dear Chairman Upton, Ranking Member Pallone, 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 today in advance of this week's Commerce, Manufacturing and Trade subcommittee hearing, "Discussion Draft of H.R. ____, *Data Security and Breach Notification Act of 2015*." On behalf of NAFCU member credit unions and the 100 million credit union members across the country, we appreciate the subcommittee's attention to this very important matter. Still, NAFCU has concerns about the discussion draft and looks forward to working with you to address them as this issue moves forward.

While we appreciate the inclusion of a national standard for data security for retailers in the discussion draft, we believe the standard must be strengthened beyond "reasonableness." Just last week we wrote to Congress to bring your attention to a recently released *Verizon 2015 Payment Card Industry Compliance Report* which found that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. Massive data breaches at our nation's largest retailers continue to put millions of consumers at risk and have cost credit unions across the country millions of dollars in fraud related investigations and losses, card reissuance costs, and additional card monitoring. While a "reasonable" standard described in the discussion draft is a good first step, without inclusion of a robust and mandated rulemaking, little will be done to prevent data breaches and protect consumers.

Also noted in the *Verizon Report*, out of every data breach they studied over the past 10 years, not one single company was in compliance with the PCI standards at the time of the breach. This should cause serious pause among lawmakers as failing to meet these standards, exacerbated by the lack of a strong federal data safekeeping standard, leaves merchants, and therefore consumers, more vulnerable to breaches. If retailers cannot be trusted to comply with contractual obligations in an ongoing manner, nothing short of a national standard with the threat of monetary penalties for noncompliance will ensure that consumers are protected from identity theft and financial fraud. NAFCU believes that this level of data security cannot be achieved by the discussion draft in its current form.

Additionally, we believe that greater clarity of who is exempt from the definition of “covered entity” in the discussion draft needs to be provided. Credit unions are already covered by Federal data protection standards and notification laws and should not be subject to dual and inconsistent regulation. We appreciate that the discussion draft attempts to address this, but we believe that this language needs to be improved upon as we are concerned that some credit unions may fall under the “covered entity” definition as the language is currently drafted.

We also urge the inclusion of language to make those entities that fail to meet a data protection standard liable for any costs incurred from a breach of their systems. At the very least, the legislation needs to ensure that credit unions and others maintain a right to seek legal redress of any costs that they incur from a data breach.

We also note the breach notification provisions contained in the discussion draft. It is important for consumers whose personal data may have been compromised to be made aware of the risk so that they can take proactive steps to ensure that their personal information is not used in a fraudulent manner. Notification, however, is a reactive approach rather than a proactive one that will prevent breaches from happening in the first place. Notification standards without robust data security standards will not help consumers protect their personal information from a breach. Furthermore, we believe it is important to clarify in the bill that credit unions should have the ability to inform their members of a data breach at another party, including where the breach may have occurred.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. The difference, however, is that credit unions have developed and maintain robust internal protections to combat these attacks and are required by federal law and regulation to protect this information and notify consumers when a breach occurs that will put them at risk—no matter what size of the institution. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to \$1 million per day for compliance violations. These extensive requirements and safeguards have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999 as part of the *Gramm-Leach-Bliley Act (GLBA)*. In contrast, retailers are not covered by *any* federal laws or regulations that require them to protect the data and notify consumers when it is breached.


The ramifications for credit unions and their members have been monumental. A February 2015 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were \$226,000 on average. Of their losses, respondents expect to recoup less than 0.5% which amounts to less than \$100 on average. Despite the claims of some trade groups, the fact remains that our members are not recovering anything close to what they are spending to make their members whole after a merchant breach.

Ultimately, NAFCU believes that any comprehensive data security legislation must address:

- **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.
- **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 *GLBA*.

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

We urge the subcommittee and authors of the discussion draft to require a robust rulemaking for national data security standards in any final draft. Anything short of this will fail to provide consumers with the identity and financial protection that they want and deserve. We look forward to working with you and your staff on this data security legislation. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Director of Legislative Affairs Jillian Pevo at (703) 842-2836.


Brad Thaler
Vice President of Legislative Affairs

cc: Members of the House Energy and Commerce Committee



March 17, 2015

The Honorable Michael Burgess
Chairman, Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
2336 Rayburn House
Washington D.C. 20515

The Honorable Jan Schakowsky
Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
237 Cannon HOB
Washington, D.C. 20510

Re: Comments on Discussion Draft "Data Security and Breach Notification Act of 2015"

Dear Chairman Burgess and Ranking Member Schakowsky,

The Online Trust Alliance (OTA) submits this letter in advance of the March 18, hearing being held by the Commerce, Manufacturing, and Trade Subcommittee on the recent draft "Data Security and Breach Notification Act," authored by Representatives Blackburn and Welch.

We commend the Subcommittee for recognizing the need to develop meaningful legislation to help protect consumers from the onslaught of data breaches and negligent data protection practices, which risk considerable harm to consumers. Indeed, for the 15th consecutive year - identity theft is the top category of consumer complaints made to the Federal Trade Commission (the "Commission"), **underscoring the need for legislation requiring responsible data security practices along with timely and actionable notices of a data breach.**¹

OTA and our members have deep experience in this subject matter, and based upon our experiences, have identified several areas for enhancement and clarification of the draft bill. These comments follow OTA's letter dated March 3, 2015, to the House Committee on Commerce, Science, and Transportation, concerning draft data breach legislation. (Attached).

¹ <https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014>

We believe a single Federal law pre-empting the patchwork of 47 State laws will benefit consumers and business alike, by providing clarity and a single standard definition of privacy, notification requirements and reasonable security requirements. **However, any federal data breach notification law must be sufficiently robust, while not unduly burdening businesses committed to protecting consumers and their data.**

Consumers today are becoming jaded and risk being overwhelmed by the sheer volume of data breach notices. Often, these notices are unclear, not prescriptive nor timely. **It is critical that any federal data breach legislation recognize that for each day a consumer is not provided actionable notification, the risk of victimization grows.**

Below is a summary of key points which we believe are essential for an effective and balanced federal data breach notification law, to pre-empt existing state laws.

1. **Covered Data** – As written, the scope of the Act only covers electronic data. However, an organization’s accidental loss or discarding of paper records containing personal information impacts consumers in the same fashion as an electronic breach. A paper data loss can result in “dumpster diving” and identity theft. In many cases, the paper data loss of consumer information can be more impactful, especially where tax returns, W-2s, bank statements, or other financial data are involved. With this in mind, we recommend that the bill be amended to include covered data in any form, whether electronic or paper.^{2, 3}
2. **Section 2 Requirements** – OTA’s independent analysis shows that more than 90% of breaches that occurred in 2014 could have been prevented and contained by adoption of best practices. OTA agrees with the concept in the draft bill that covered entities must maintain reasonable security measures to protect and secure personal information. While there is no perfect security, prevention is only one facet of data protection. As outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity, covered entities must also deploy processes to help detect a data loss incident, as well as formulate measures to contain and minimize the impact of a data breach incident.⁴ Equally as important, a covered entity must have an up-to-date data breach response plan. All too often we have witnessed organizations failing to have such a plan, delaying timely notices to the consumer. The draft bill should be amended to include these requirements and to afford “safe harbor” treatment from violations and fines for those entities who can demonstrate they have implemented said best practices in their respective areas.

² <http://recode.net/2015/03/10/dumpster-divers-could-be-the-next-sony-hackers/>

³ <http://www.click2houston.com/news/tax-documents-found-in-dumpster/30932828>

⁴ <http://www.nist.gov/cyberframework/index.cfm>

3. **Notification** – There are three primary facets of notification that are required to maximize consumer protection and help defend our nation from cybercrime. These are: (1) regulatory authorities (the Commission), (2) law enforcement, and (3) consumers and other impacted parties (e.g. partners, investors, etc.). Section 3(a)(3) specifies a “covered entity shall as expeditiously as possible notify the Commission and the Secret Service or the Federal Bureau of Investigation.” Based on recent notifications that have lagged upwards to six months or greater, it is recommended that the draft bill specify notice to the Commission and Law Enforcement be within seventy-two hours (3 business days) after discovery of a breach or data loss incident involving personal information. It is recognized the full impact of the incident may not be known and the reporting entity will likely revise their findings, but delaying notification until an internal investigation is complete impedes the efforts of the law enforcement community and first responders.
4. **Non-Profit Entities** - As written, the draft bill only addresses 501(c)(3) charitable organizations and reduces their notification requirement. OTA strongly believes all non-profit organizations should be classified as covered entities. We have witnessed trade organizations, religious organizations, and others experiencing data breaches resulting from insecure storage of personal information.^{5 6} All organizations that hold and collect personal information must be held to the same standards for both protecting covered data and providing notifications.
5. **Method and Content of Notifications** – The draft bill in Section 3(d)(1)(ii)(III) recognizes that data breach notifications should be constructed so they do not become an attack vector, by not containing any hyperlinks. It is important to recognize there are other measures that must be in place as well to help prevent consumers from receiving dubious and look-a-like notices, as experienced in the recent Target breach. In the absence of rulemaking provisions for the Federal Trade Commission, it is recommended this section be expanded to include two critical requirements: 1) notices should only come from the recognizable domain and consumer facing brand of the covered entity; and 2) the covered entity must implement anti-spoofing and phishing standards to aid internet service providers and receiving networks to help detect and block phishing and malicious email.^{7, 8, 9}
6. **Content of Notification** – Notifications that include detailed information are extremely important to aid consumers to be able to take action to protect themselves. Section 3(b) should add an additional provision requiring the notification to include the physical location of the breach, if known. For example in last summer’s Jimmy Johns breach, the precise location and date of the incident was made known to customers. Providing this information enabled Jimmy John’s customers to quickly determine if their credit card was compromised.

⁵ <http://www.komonews.com/news/local/Victims-of-IRS-tax-fraud-continues-to-grow-250407271.html>

⁶ <http://www.net-security.org/secworld.php?id=13669>

⁷ <http://mainsleaze.spambouncer.org/target-spams-email-appended-list-with-data-breach-notice/>

⁸ Email Authentication Best Practices <https://otalliance.org/eaauth>

⁹ <https://otalliance.org/EmailAudit>

The draft bill should be amended to state when known, the physical location(s) should be included and disclosed to the consumer in the notification.¹⁰

7. **Notice Requirement of Service Providers** - Timely notification by service providers to covered entities is critical. As businesses are becoming more reliant on service providers, this risk is increasing, yet there is no such standard notification timetable for service providers. **Service providers often do not know the types of data they are holding, have access to the data and/or may be contractually prohibited to know what data they may be holding.** In the absence of this knowledge, they do not know if they need to notify the customer unless it has been contractually stipulated. For this reason, it is recommended service providers be required to notify the covered entity within forty-eight hours of the detection of a breach, data loss or possible incident impacting the service they are providing to a covered entity.
8. **Covered Data** – The draft bill in Section 5(A)(iii) does not appear to include in the definition of personal information unique identifiers related to email, social networking accounts, dating, and other online services. The breach of these kinds of accounts can be drivers of identity theft and phishing. To maximize consumer protection, it is recommended the section be clarified to include any log-in credentials including a unique account identifier and associated security code, access code, password, or biometric data unique to an individual. Highlighting the importance of this clarification is the use of federated ID mechanisms outlined by the National Strategy for Trusted Identities in Cyberspace (NSTIC)¹¹ and federated sites using Facebook login credentials.¹² As defined in the draft bill, it is unclear if these account identifiers and security codes would be covered. To maximize consumer protection and harmonize with existing state breach laws, such accounts and credentials must be covered.
9. **Sharing of Investigative Data with Law Enforcement** - The draft bill does not provide any safe harbor for covered entities that share investigative reports or forensic data with law enforcement. The lack of a safe harbor from federal or state laws risk can impede the sharing of this critical information and threat intelligence. When such sharing is used exclusively for law enforcement investigative purposes it should not constitute a violation of federal or state law as well as a covered entity's privacy policy. Sharing forensic data as soon as possible can be invaluable to aiding law enforcement to help protect others and ultimately bring criminals to justice. Thus, the sharing of such data, including investigative reports and forensic data, should be encouraged through appropriate protections in breach legislation.

¹⁰ <https://www.jimmyjohns.com/datasecurityincident/>

¹¹ <http://www.nist.gov/nstic/>

¹² <https://developers.facebook.com/docs/facebook-login/v2.2>

10. Maximum Total Liability – The draft bill in Section 4 imposes an unreasonably low penalty amount for violations which could not be reasonably expected to deter misconduct or redress tangible harms to consumers. We recommend that covered entities who fail to comply with Section 2 and are unable to demonstrate they have implemented reasonable security to help prevent, detect and contain an incident, should have a maximum civil penalty for each violation not to exceed \$20,000,000. This would be consistent with recent breach related settlements with multiple State Attorneys General.¹³

In summary, OTA applauds the Subcommittee in taking leadership in this critical area. We look forward to working with members in developing effective legislation that maximizes consumer protection, promotes innovation and aids in fighting cybercrime.

Sincerely,



Craig D. Spiegle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
+1 425-455-7400

cc: House Commerce, Manufacturing and Trade Committee Members

¹³ http://www.dispatch.com/content/stories/business/2009/06/23/timax_settlement.html



March 3, 2015

Chairman Fred Upton
U.S. House of Representatives Energy & Commerce Committee
2183 Rayburn House
Washington D.C. 20515

Ranking Member Frank Pallone, Jr.
U.S. House of Representatives
237 Cannon HOB
Washington, D.C. 20510

Re: Proposed Data Breach Notification Legislation

Dear Chairman Upton and Ranking Member Pallone:

The Online Trust Alliance (OTA), a 501c3 non-profit with the mission to enhance online trust and promote innovation, submits the following in response to the recently announced Personal Data Notification & Protection Act and several related draft legislative proposals.

OTA represents over 100 organizations committed to the development and advancement of best practices, meaningful self-regulation, data stewardship and balanced legislation. Last month, OTA released its 2015 Data Protection & Breach Readiness Guide developed through feedback from over 100 security and privacy professionals, and held four town halls around the United States where over 500 attendees provided input concerning the various data breach notification proposals. America's leadership is being threatened and data breaches are a challenge to national security, the economic prosperity of our nation, and most importantly, to the privacy and financial protection of our citizens.

Below is a summary of six key points and provisions which we believe are important considerations for an effective and balanced federal data breach notification law.

First, any federal data breach notification law must preempt the existing 47 state laws imposing a myriad of data breach notification obligations. State breach laws are a complex web of varied timing and notification requirements, and are a difficult mish-mash for an inter-state business to navigate during the challenge of responding to a data breach incident. Similar to the single data breach notification requirement in the EU, a single federal law will provide

businesses, consumers and regulators with clarity and simplicity concerning data breach notification obligations and provide a level playing field for all consumers – no matter their state of residence. However, any federal data breach notification law must be robust and not provide lesser protections than under existing state laws while not unduly burdening businesses.

Second, any federal data breach notification law must contain a safe harbor from regulator penalties for those businesses or organizations that can demonstrate a commitment to the adoption of best security and privacy practices. While it is important to recognize there is no perfect security, OTA's analysis of data shows that more than 90% of breaches that occurred in 2014 could have been prevented by adoption of best practices. A safe harbor from penalties for self-certified adoption of best practices would strongly encourage businesses to adopt best practices when they are most needed - in advance of a breach.

Third, any federal data breach notification law must contain a State right of enforcement. Similar to the Children's Online Privacy Protection Act (COPPA) and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), a state right of enforcement not only permits a state to protect its own citizens, but also allows states to complement the overburdened federal regulators by pursuing those companies and organizations that fail to live up to their data breach obligations. States have a strong interest in protecting their own citizens and a federal data breach notification law with a State right of enforcement would recognize and embrace this interest.

Fourth, any federal data breach notification law must contain an appropriate coverage of personal information triggering notification obligations. This is critical to ensure consumers are notified in a timely manner and for those breaches they need to know about, and are not over notified. If notifications become commonplace, consumers will get lost in the noise and likely not take appropriate action. Thus, the definition of what data is covered must be balanced and appropriate, must include paper records, and due to the common reuse of passwords by consumers across their numerous accounts – must include coverage for email/username address and passwords. A user's email address and password are essentially the keys to their online kingdom, permitting access to social and financial websites, either directly or through a master account password reset.

Fifth, timely notice is critical to not only consumers, but also to regulatory authorities and law enforcement agencies. Businesses should be required to notify the FTC, FCC or other primary regulatory within seventy-two hours after discovering a breach involving covered data. Since the window of consumer victimization begins within days of a breach, it is critical that businesses notify consumers as soon as possible - but no later than 30 days after a breach. While breach investigations are complex and take time, they often identify additionally impacted consumers weeks later. With this in mind, any data breach legislation must provide for a rolling period of notification not to exceed 30 days after discovery that a consumer's personal information has been breached.

Sixth, any data breach legislation must permit businesses to share investigative forensics reports and related data with any law enforcement agencies investigating a breach. This sharing should not constitute a breach under the legislation nor impact any privilege or protections belonging to a business. Sharing forensic reports and data as soon as possible concerning a breach and attempted breach can be invaluable to help protect others and bring attackers to justice, or should be encouraged through appropriate protections in any data breach legislation.

OTA applauds Congress and the President for taking leadership in this critical area. As an individual's online worlds grows and expands, as our next generations spend more and more time socializing, communicating, gaming, shopping, banking, and researching online, so must the protections afforded to them.

We look forward to working with your staff and colleagues in the developing effective legislation which maximizes consumer protection and promotes innovation and fight the threats which our undermining the interest and our economy.

Sincerely,



Craig D. Spiegle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
+1 425-455-7400

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
MARCH 18, 2015
“Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015”

Chairman Burgess, 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.

We submitted testimony for the subcommittee's January 27th hearing on the elements of sound data breach legislation which laid out the interest our members have in data breach legislation, noted how the payment card system impacts our data security efforts, provided background on data breaches, explained the current state of the law on data breach notification, and walked through the elements of data breach legislation that we consider to be most important.

This statement will focus on the draft "Data Security and Breach Notification Act of 2015" (Draft Bill).

A Central Concern with the Draft Bill

The Draft Bill sets a federal framework for data security standards for U.S. businesses and a system of notification requirements in the event that data breaches occur. The Draft Bill establishes a reasonableness standard that businesses must meet with respect to data security and, in our view, that makes sense given the wide diversity of businesses and circumstances that the Draft Bill aspires to cover. We do have concerns that this data security standard exempts some types of businesses from its coverage and that many of those businesses are not required by any

other laws to maintain a reasonable level of data security, but we will address that issue later in this statement.

Our overriding concern about the Draft Bill is that it creates fundamental problems that seem to undermine the intentions of its authors by taking large categories of U.S. businesses and foisting their notification obligations (with attendant threat of enforcement and fines) onto other U.S. businesses. The Draft Bill categorizes some businesses as “third parties” and others as “service providers.” Third parties, as defined by the bill, store, process, maintain, transmit or route data on behalf of other businesses. These third parties include internet and other technology companies, cloud storage providers, payment card processors, payment card networks and many others. Companies that meet the definition of third party for much of the business they conduct include many corporate giants and household names such as Google, IBM, Oracle, Toshiba Samsung, Automatic Data Processing (ADP), Visa, MasterCard, and First Data.

Service providers are defined in the Draft Bill as businesses that transmit, route, or provide intermediate or transient storage of data for another business and are covered by the Telecommunications Act. Service providers also include corporate giants and household names such as Comcast, Verizon, and AT&T.

Under the Draft Bill, third parties and service providers do not need to notify affected consumers or the public when they have a data breach. In fact, in some situations, service providers do not need to notify anyone at all when they have a data breach. In other situations, the third parties and service providers are only required to notify the businesses whose data was taken in the breach. Then, according to the Draft Bill, once a business has been told by a third party or service provider that some of its data has been breached, all of the responsibility and cost of notifying affected consumers and the public along with the risk of enforcement by the Federal Trade Commission (FTC) and state attorneys general and attendant fines running into the millions of dollars fall on the business that was notified – not the business that suffered the data breach. That is fundamentally unfair. And, to the extent that requiring businesses to provide notification of their breaches incentivizes those businesses to try to protect against such breaches, that incentive is lost for third parties and service providers under the bill.

NACS and SIGMA, for example, collectively represent tens of thousands of single store operators whose pre-tax profits average about \$47,000 per year. These businesses are not unique. There are many small businesses across the country in many different areas from restaurants to small shops, corner grocery stores, doctors’ offices, and individual entrepreneurs that similarly work very hard just to make ends meet each year (or each pay period). But the service provider provisions of the Draft Bill mean that if Comcast, for example, suffers a breach of its data lines the most it has to do is notify businesses like a mom-and-pop convenience store whose data may have been carried when the breach occurred. Then, mom-and-pop convenience store is on the hook for complying with all the notification provisions of the Draft Bill and will face large fines if it doesn’t do it right even though Comcast had the data breach. The same is true for third parties – just substitute Visa or Google for Comcast.

This is fundamentally unfair. Corporate titans should not be able to foist legal responsibility for notifying people of their own data breaches onto businesses that did not have a

data breach at all. The same would be true even if the third parties and service providers involved were universally small businesses. The cost and legal peril shifted onto other businesses simply does not make sense and those businesses have little if any ability to influence the data security practices of the third parties and service providers with which they deal.

Some have argued that third parties and service providers need to pass their notification responsibilities onto other businesses because consumers might not do business directly with those third parties/service providers and might otherwise be confused. First, we would note that consumers have a wealth of experience dealing directly with telecommunications companies (service providers), understand what services they provide, and likely would not be confused by receiving notices from them about their data breaches. Second, many third parties are equally recognizable (e.g., Visa/MasterCard) and would not engender any confusion by providing notices. Third, in situations for which there might be a genuine confusion problem, there is nothing in the Draft Bill or elsewhere that would prevent an explanation of how the data breach connects directly to the consumer involved (such as by noting that the business providing the notice handles data on behalf of a local business with which the consumer transacted). That explanation would be much less confusing in many instances coming from a business that actually suffered the data breach than coming from a business that did not suffer a breach (whose veracity may unfairly come into question simply because it provided the notice).

It is also worth pointing out that, during the subcommittee's hearing on January 27th on this topic, Representative Gus Bilirakis (R-FL) asked the panel which business should bear the notice responsibility in the event of a data breach. Jennifer Glasgow, Chief Privacy Officer of Acxiom, Brian Dodge, Senior Vice President of Communications and Strategic Initiatives for the Retail Industry Leaders Association (RILA), and Woodrow Hartzog, Associate Professor for the Cumberland School of Law, all answered that the business suffering the breach should bear the responsibility of providing notice to affected consumers. Only the witness representing a trade association for the information technology industry, whose members include many businesses defined as third parties and service providers by the Draft Bill, differed with the other witnesses on that point.

Having third parties and service providers pass their notification responsibility onto bystander companies creates many other problems – some of which do not make sense and were likely not intended by the bill's authors. We walk through just some of most glaring of those problems below, but we urge you to resist the strong temptation to simply try to patch over each of these problems individually. These issues are not the problem. They are symptoms of the underlying problem that many businesses which have a data breach are able to foist legal and financial responsibility for notification of that breach onto other businesses. New drafts of the bill cannot overcome these issues without creating new ones unless and until the treatment of third parties and service providers is fundamentally changed so that they remain responsible for notification in the event of their own breaches. Attempting to treat the individual issues pointed out below would be like building a hull of a ship with half of the necessary boards missing – and then trying to patch the gaps like they were individual small leaks. The job will never be completed to allow such a ship to float. The hull needs all of its boards to be sound.

And here, all businesses that suffer data breaches need to have responsibility for notifying affected consumers and/or the public or a federal data breach scheme will never work as well as it should.

Individual Problems Created by the Separate Treatment of Third Parties

As noted above, third parties only need to inform the business for which they store, process, maintain, transmit or route data of the information that was breached and then the notified business (that was not breached) has to provide notice to affected individuals. That leads to the following problems:

- **Individual notice may be impossible** – if the information that was breached does not include contact information for the affected individuals, the breached business has no responsibility to provide contact information so individual notice may be impossible. That means substitute notice (by posting on the website of the business that did not have a breach) may be the only possibility.
- **Notice may not be timely** – third parties are only required to provide notice to the non-breached business “promptly.” But the non-breached business is required to provide notice to affected individuals within 30 days after the breached system has been restored.
 - But the non-breached business might not be aware of the breach within 30 days of the system being restored (it’s not clear how long “promptly” is).
 - And, the non-breached business might not know when it is required to provide notice because the breached business has no obligation to tell it when the breached system has been restored (and might want to keep that information confidential).
 - Despite these problems, the business that did not even suffer a breach is subject to fines under the FTC Act and penalties from state Attorney General lawsuits of up to \$2.5 million if it does not provide timely notice of a breach – even if it was not aware of the breach before the deadline and/or was not aware of what the notice deadline was.
- **Key information may never be known** – third parties are not required to perform any investigation if they have a breach (breached businesses other than those defined as third parties or service providers are required to do so). So, there is no way for the non-breached party to determine whether there is a risk to consumers that should lead to notice and important information about the causes and extent of the breach may never be known.

Individual Problems Created by the Separate Treatment of Service Providers

As noted previously, a business that transmits, routes, or provides intermediate or transient storage of data for another business and is covered by the Telecommunications Act is a “service provider” and does not need to notify individuals when it has a data breach. Service providers have fewer responsibilities than third parties.

- **No notice to anyone** – service providers do not need to notify anyone when they have a breach unless they can “reasonably identify” the business that was sending the

information that was breached. But service providers have no obligation to conduct any investigation or inquiry into their data breach in order to identify the business sending the information. The result is likely to be that no one is informed of anything in many instances when a service provider has a data breach.

- **Notice may not be timely** – there is no timing by which service providers must notify non-breached businesses of breaches (it doesn't even have to be "promptly" as with third parties). That exacerbates the problems with notice timing. Non-breached businesses may in many circumstances not be aware of a breach at a service provider until after they were required to provide notice of that breach. Non-breached businesses, however, will potentially be subject to fines under the FTC Act and state enforcement with penalties of up to \$2.5 million for not providing notice of breaches they did not have and were not aware of until after the deadline for notice.
- **Key information may never be known** – service providers, like third parties, are not required to perform any investigation if they have a breach (other breached businesses are required to do so). So, there is no way for the non-breached party to determine whether there is a risk to consumers that should lead to notice and important information about the causes and extent of the breach may never be known.

Consumers Will Receive Multiple, Confusing Notices of Many Third Party and Service Provider Breaches

By making non-breached businesses provide notice when third parties or service providers have breaches, the draft bill will lead to individual consumers receiving multiple notices regarding the same data breaches. Those notices will include different contact information and risk both confusing and alarming consumers. The multiple notices will also lead to unnecessary, duplicative costs on businesses.

- **Multiple Notices of Telecommunications Breaches** – when a telecommunications provider has a breach, it is likely that the data of multiple businesses sending data over the telecommunications system are impacted. There will be many instances in which those businesses have some overlap in customers (those customers are likely, for example, to do business with multiple local businesses and not just one). The telecommunications company, however, may tell all of the multiple affected businesses of the information that was breached (if, as noted above, they tell anyone at all) and each of those non-breached businesses will be responsible for notifying their customers. So, it would not be surprising for an individual consumer to receive notices from the local restaurant, hardware store, grocer, drug store, and convenience stores regarding the same breach. And these notices will include some of the same along with some different contact numbers. They might also describe the information and circumstances differently leading to additional confusion.
- **Multiple Notices of Payment Processor/Network Breaches** – when payment processors (such as First Data) and networks (such as MasterCard) have breaches, it is highly likely that the data of multiple businesses sending payment card transactions over their systems are impacted. The results for these "third party" breaches will be much the same as for the telecommunications "service providers" noted above. Multiple affected

businesses may be notified and they, in turn, will each have to notify their customers – many of whom will be the same because they shop at multiple different businesses.

Third Parties, Service Providers and Others Will Have Non-Existent (or Reduced) Notice Obligations

Even though third parties and service providers are only required to notify the non-breached business(es) of their breaches, those third parties and service providers will no longer have to comply with state data breach notification laws under the pre-emption provision of the draft bill. This reduces the notice obligations of these companies under current law. And, for service providers, they will not have to investigate when they have a breach and will not need to notify anyone if they don't know who sent the data (which is likely without investigation).

- **The result of the draft bill for service providers, then, is that they could have a breach, not investigate at all, not notify anyone, and not have to comply with any of the 47 state data breach notification laws.**
- Similarly, banks and credit unions are not covered by the data breach notification provisions of the draft bill and will not be required to investigate breaches or notify anyone of their breaches under the Draft Bill. They do have guidelines under the Gramm Leach Bliley Act (GLBA) that say they “should” notify consumers when they have breaches, but that guidance is written in discretionary terms and is not required. The disparity in notice obligations between these financial institutions and the businesses with which they exchange data millions of times per day will lead to vulnerabilities that data thieves will exploit to steal data (and keep the thefts secret for as long as possible).

Many Businesses May Be Falsely Blamed for Breaches They Did Not Have

The Draft Bill allows businesses to contract with another business to provide notice. This makes sense because, especially in many large breaches, it is much more efficient and leads to more effective notice if a business that specializes in providing these types of notices is used. The problem comes when there are third party or service provider breaches.

- **Non-breached businesses must be blamed** – when a third party or service provider is breached, a non-breached business has the legal responsibility to provide notice (assuming the service provider notifies anyone at all). But the provision allowing a contractor to send the notice requires that the notice say that it is being provided on behalf of the business that contracted for the notice to be sent. That means the notice must blame the non-breached business for the breach, even though the breach was of a third party or service provider. So, the draft bill saddles the non-breached business with the legal obligation and costs of providing notice under the threat of fines and, if it uses a contractor to provide notice, requires the non-breached business to take the blame for the data breach.

Enforcement Will Unfairly Focus on the Wrong Businesses

As noted above, businesses that are informed by third parties and service providers of breaches at those third party and service provider businesses will be subject to enforcement even though they did not suffer a data breach.

- **Penalties without breaches** – Businesses that did not even have a breach will be subject to FTC enforcement and penalties under the FTC Act as well as state AG enforcement with penalties of up to \$2.5 million.
- **Penalties without a chance to comply** – Businesses that receive notice from third parties or service providers close to or after 30 days from the time the third party or service provider's system is secured will have no way to comply with the draft bill, but will still be subject to enforcement by the FTC and state AGs and fines for non-compliance.

Financial Institutions Will Not Have Data Security or Data Breach Notification Obligations Under the Draft Bill

One other issue that bears attention is the exclusion of banks and credit unions from the Draft Bill. These institutions are certainly vulnerable to data breaches. In fact, according to the most recent Verizon Data Breach Investigations Report, financial institutions have about three times as many breaches as do retailers. Banks and credit unions exchange payment card information with businesses fully covered by the bill as well as third parties and service providers hundreds of millions of times per day. Those banks and credit unions do have guidelines under GLBA that say they "should" have data security processes and procedures in place, but that guidance is written in discretionary, not mandatory, terms.

Having banks and credit unions subject to permissive guidelines on data security and data breach notification while the other businesses with which they exchange data are subject to requirements backed by FTC and state AG enforcement invites differential standards and data vulnerabilities. Data thieves do not limit their activities to any one category of business. They go after everyone and are successful in every category. The Draft Bill should cover everyone if it is meant to improve our preparedness for and reactions to data thieves' activities.

* * *

We appreciate the subcommittee providing us with this opportunity to submit our views on the Draft Bill. We look forward to working with you as the committee continues to consider this topic.

March 18, 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

Statement for the Record for the Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade Hearing
On the Data Security and Breach Notification Act of 2015

Dear Chairman Burgess and Ranking Member Schakowsky:

Thank you for holding a hearing on the Discussion Draft of the Data Security and Breach Notification Act of 2015.

We share your concerns about protecting consumers and submitted a joint letter on January 23, 2015 in advance of your Subcommittee hearing on this issue. Our letter outlines a set of principles to serve as a guide when drafting legislation to provide stronger protection for consumer financial information. For more than 15 years, the financial industry has been subject to significant regulatory requirements and internal safeguards which have been substantially enhanced over the years, and we commend you on moving forward with legislation that is intended to increase consumer protection by encouraging greater protection of sensitive personal and financial information.

We look forward to working with you in a constructive way on the Discussion Draft. However, we have concerns about the Draft and believe that it would be improved by the following modifications:

Requirements for Information Security

Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security bill and these standards should be applicable to any party with access to important consumer financial information.

The Discussion Draft takes a step forward by including data protection requirements in Section 2. However, the current “reasonable security measures” standard set forth in this draft would be strengthened by including flexible and scalable standards similar to those applied to financial institutions through the Gramm-Leach-Bliley Act (GLBA) and its subsequent rules and regulations.

Since this draft does not include an FTC rulemaking requirement, it is especially important that meaningful data protection standards be included in the bill. In addition, since the bill preempts state laws, and because we are obliged to support a standard that protects consumer information

throughout the entire supply chain, we believe a strong data security requirement would help protect against the unintended consequence of providing consumers with less protection than afforded under current law.

Current GLBA standards require entities that acquire personal and financial data to put in place a process to protect that data. It does not mandate specific technology, but the extent to which entities need to ensure the information is protected is based on the size and complexity of the entity, the activities the entity undertakes, and the sensitivity of the information being held.

Definition of “Covered Entity”

Banks and credit unions are already subject to robust data protection and notification standards under the GLBA. These requirements must be recognized in legislation and entities already covered by Federal data protection and notification laws and regulations should not be subject to dual and perhaps inconsistent regulation.

We therefore appreciate the Committee’s efforts to ensure no industry is burdened by unnecessary duplicative regulation, and the Discussion Draft appears to address this, at least in part. However, the language included in Section 5 may not be broad enough to completely exempt those already covered by GLBA data protection and notice provisions. In particular, state-chartered credit unions, certain non-bank subsidiaries of banks and bank holding companies and affiliates of credit unions may be subjected to dual oversight and enforcement. Subsequently, because such entities are also governed by their parent companies’ regulatory requirements, this could effectively subject them to dual regulation. We look forward to working with the Committee to solve this problem.

Preemption of State Law

Inconsistent state laws and regulations specifically dealing with data protection and consumer notification should be preempted for all entities that are subject to strong Federal data protection and notification standards, whether they are considered “covered entities” within the meaning of the Discussion Draft or covered by other laws such as the GLBA. As drafted, Section 6 does not accomplish this.

Consumer Notification

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. Section 3 of the Discussion Draft contains detailed notification requirements. However, this section should also be modified to clarify that 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.

Costs of Breach

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. Section 4 of the Discussion Draft should be modified to reflect this. Specifically, an entity that fails to comply with the data protection requirements of Section 2 that experiences a breach involving sensitive account information would be liable for any losses resulting from the breach and for any reasonable costs to protect the accounts.

We look forward to working with you and your colleagues on the Energy and Commerce Committee, as well as other Committees, such as the Financial Services Committee, to craft data protection and notice legislation to better protect your constituents' personal financial information.

Sincerely,

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

**Secret Service Answers to
Questions regarding Data Breaches from
Energy and Commerce Committee, U.S. House of Representatives
19 February 2015**

Background: The Committee is continuing to examine the commercial data breach landscape, particularly with the number of high profile breaches in the news over the last few years.

- 1) Given the Secret Service's extensive history with financial fraud and data breach investigations, I am wondering if you can confirm that the majority of commercial data breaches are monetized through credit card fraud or identity theft?***

Data breach trends are difficult to confidently measure given low detection and reporting rates. In addition, agencies, including the Secret Service, are inherently biased in observing incidents within their jurisdiction. To overcome this bias, the Secret Service has been a partner, since 2009, in producing the Annual Verizon Data Breach Investigations Report (DBIR).¹ The DBIR is widely regarded as the authoritative source regarding data breach trends.

The 2014 DBIR analyzed 63,347 cyber security incidents in 2013, including 1,367 confirmed data breaches, and showed that over 60% of confirmed data breaches were attributable to a clear financial motive. Additionally, this report shows that from 2011-2013, Point-of-Sale Intrusions have been the largest type of data breach. —All such data breaches are monetized through credit card fraud and identity theft. Based on the analysis of data in the DBIR and other cyber reports, it is the Secret Service's estimation that the majority of data breaches are primarily monetized through financial fraud.

The 2015 DBIR is currently being drafted and is planned for release this spring. Once it is released, the Secret Service is available to arrange a briefing on the findings of the 2015 DBIR.

- 2) In terms of impact for individual consumers – do these seem to be the most significant harms?***

Data breaches for the purposes of financial fraud appear to have the greatest impact on individual consumers. Additionally, they are highly significant because the perpetrators are able to monetize their activity and reinvest their proceeds to further develop their criminal organizations and capabilities. Current academic research² supports the claim that

¹ Available at: www.verizonenterprise.com/DBIR/

² See, for example: Anderson, et al. "Measuring the Cost of Cybercrime." Workshop on the Economics of Information Security WEIS 2012 (June 2012). Available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

financially motivated cyber incidents have the greatest economic significance on consumers.

3) *Are there other significant harms that are impacting individual consumers from these large scale breaches?*

Financial institutions are generally responsible for all fraudulent purchases involving stolen payment card data. However, fraud losses and administrative costs to combat cyber crime are likely passed on to merchants and consumers in the form of higher transaction fees. Additionally, consumers often spend time and in some instances money monitoring their accounts or credit reports for suspicious activity to report to their financial institutions. Finally, the intangible cost to consumers - fear that their data may be stolen - may result in negative consumer adaptations.

4) *What else do criminals use the data stolen from breaches for?*

There is a robust underground market for stolen information and criminals are increasingly developing new means to profitably exploit this data. For example, they may sell lists of stolen email addresses to spammers or sell username/password combinations to enable other data breaches. Criminals may also use the knowledge of a data breach as part of complex fraudulent schemes to profit on the change in a company's stock price when the information of a breach becomes public (e.g. by shorting a stock). Cyber criminals are quickly increasing in sophistication and progressively developing new means to exploit stolen data for profit or to further their criminal enterprises.

5) *How often is geolocation information targeted in these attacks?*

Geolocation information is often collected in data breaches. However, the Secret Service has not observed criminal schemes directly profiting from geolocation data. This is a possible explanation as to why it has not been a primary target in most data breaches.

6) *If geolocation information is breached, what is the value for the criminals? How are they using that information?*

Associated geolocation information may increase the value of stolen data for criminals in some cases. Geolocation data can be used to defeat some fraud detection measures used within the payment card industry. Additionally, some purchasers of stolen data may be interested in the associated geolocation information for marketing purposes or to target particular individuals or organizations through complicated schemes.

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 (702) 225-2927
Minority (702) 225-3941

July 13, 2015

Ms. Jessica Rich
Director
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

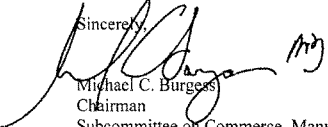
Dear Ms. Rich,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015."

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 with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

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

Additional Questions for the RecordThe Honorable Michael C. Burgess

1. Under the FTC's current authority, the Commission must obtain a consent order before it can obtain civil penalties for unfair or deceptive data security practices. Do you believe that consent orders are a strong incentive for industry to implement data security verses civil penalties?

As you note, the Commission's data security consent orders allow for the imposition of civil penalties for order violations, and may also provide additional requirements, such as auditing and compliance obligations. These orders send an important message to the marketplace about reasonable data security. Nonetheless, we believe the impact of our orders would be stronger if we had the authority to seek civil penalties in appropriate cases for initial violations of Section 5 of the Federal Trade Commission Act. Civil penalties are an important tool to deter unlawful conduct. Accordingly, the Commission supports the provision of H.R. 1770 that gives us the ability to seek civil penalties.

Under current laws, the Commission only has the authority to seek civil penalties for data security violations with regard to children's online information under the Children's Online Privacy Protection Act, or credit report information under the Fair Credit Reporting Act. Allowing the FTC to seek civil penalties for *all* data security and breach notice violations in appropriate circumstances will help to provide better incentives for companies to maintain reasonable data security.

2. Does section 6(d) of H.R. 1770 preserve the FTC's Section 5 authority to bring unfair or deceptive acts or practices claims? Does the draft legislation preserve the FTC's Section 5 authority to bring claims for unfair or deceptive privacy practices?

Yes, I believe that section 6(d) of H.R. 1770 makes clear that the FTC's existing Section 5 authority will not be limited by H.R. 1770. We appreciate the Committee's efforts to preserve the Commission's authority to challenge unfair or deceptive acts or practices in the marketplace.

3. What factors are statutorily required for the FTC to consider when determining a penalty amount under its existing authority?

Under Section 5 of the FTC Act, the Commission has authority to obtain civil penalties for knowing violations of rules and cease and desist orders respecting unfair or deceptive acts or practices. *See* 15 U.S.C. § 45(m). When asking a court to impose a civil penalty for a proven violation, we look at a variety of statutory factors in determining the appropriate level of civil penalties to request, including the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require. *See* 15 U.S.C. §45(m)(1)(C). Ultimately, a federal judge would determine the penalty amount.

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) 225-3841

July 13, 2015

Mr. Jon Liebowitz
Co-Chairman
21st Century Privacy Coalition
1634 I Street, N.W. Suite 1200
Washington, D.C. 20006

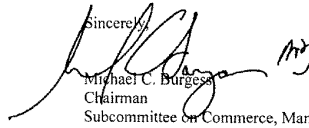
Dear Mr. Liebowitz,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015."

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 with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

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

[Mr. Leibowitz did not answer submitted questions for the record by the time of printing.]

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 (201) 226-2927
Minority (202) 225-3541

July 13, 2015

Ms. Sara Cable
Assistant Attorney General
Consumer Protection Division
Office of Attorney General Maura Healey
Commonwealth of Massachusetts
1 Ashburton Place
Boston, MA 02108

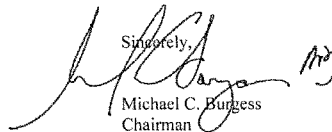
Dear Ms. Cable,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015."

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 with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

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



MAURA HEALEY
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

TEL: (617) 727-2200
www.mass.gov/ago

April 15, 2015

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

Re: *The Data Security and Breach Notification Act of 2015*

Dear Ranking Member Schakowsky:

Thank you for your questions regarding certain provisions of *The Data Security and Breach Notification Act of 2015* (H.R. ____ (March 20, 2015 Discussion Draft) (the "Bill"). We appreciate the opportunity to respond to them, and hope our responses are helpful to the Committee as it considers the Bill.

1. *What are the potential implications of the Bill's preemption clause (section 6(a)) with regard to the States' and, specifically, Massachusetts' ability to "maintain, enforce, or impose or continue in effect" laws, regulations, or standards relating to the security of data in electronic form and/or notification following a breach of security?*

Section 6(a) of the Bill restricts the States from "adopt[ing], maintain[ing], enforc[ing], or impos[ing] or continu[ing] in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a breach of security." Read in a manner consistent with the stated purpose of the Bill – to "establish[] strong and uniform data security and breach notification standards for electronic data in interstate commerce" (Bill, § 1(b)) – Section 6(a) preempts the States from enforcing or enacting data security standards (such as Title 201 of the Code of Massachusetts Regulations, section 17.00 *et seq.* ("201 CMR 17.00") or breach notification laws (such as Mass. Gen. Law ch. 93H)).

The scope of Section 6(a), however, goes far beyond the stated purpose of the Bill. Because of the breadth of Section 6(a), it could be asserted in an attempt to preempt – or at best, complicate or discourage – States' efforts to enforce existing civil or criminal laws or even enact



new laws necessary to protect its citizens or address purely local concerns, to the extent such laws are even tangentially related to data security, privacy or breach notification.

For example, Section 6(a) could be asserted by entities engaged in unfair or deceptive trade practices to thwart a civil law enforcement action by a state Attorney General under state consumer protection law (e.g., Mass. Gen. Law ch. 93A), where such practices arguably “relat[e] to . . . the security of data in electronic form.” Such practices could include, for example, solicitations in the form of false or misleading data breach notices that fraudulently induce consumers to pay for unnecessary or illusory fraud protection services or data security services, or to disclose even further personal information. With the increasing threat and ever-evolving nature of data security risks, state consumer protection laws provide vital flexibility and a vehicle by which the States can rapidly and effectively respond to protect their consumers. As drafted, Section 6(a) could present a legal hurdle complicating, unnecessarily delaying, and potentially blocking the States from enforcing their consumer protection laws to protect their consumers.

Additionally, insofar as Section 6(a) would restrict a State from “continu[ing] in effect any . . . duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a breach of security,” it could complicate a state Attorney General’s ability to enforce consumer protections obtained through prior enforcement efforts or established by prior judicial precedent. For example, a state Attorney General may face challenges enforcing compliance with data security protections required by prior judgments (or by an “Assurance of Discontinuance” or “Assurance of Voluntary Compliance” accepted by an Attorney General in lieu of initiating a civil action). Additionally, the data security standards established by such judgments and Assurances would lose their normative force. Further, the phrase “duty, requirement, standard, or other provision having the force and effect of law” could be interpreted to abolish state judicial precedents under either specific state data security or breach laws or even state common law.¹ As a result, the Bill could leave both public and private parties with little choice but to “start over” and establish new case law altogether through protracted and expensive legal action, which is not in the best interest of consumers or businesses.

Moreover, in attempting to preempt the entire field “relating to or with respect to the security of data in electronic form or notification following a breach of security,” the reach of Section 6(a) could extend to laws that impose no data security or breach notice standard, but which arguably still “relat[e] to” data security or breach notification. For example, Section 6(a) could be asserted by a criminal defendant against charges of unauthorized access to a computer system² or the interception of wire communications.³ It could also reach and potentially preempt

¹ Although Section 6(b) (which is still under debate by the Subcommittee) purports to clarify that the preemption “section shall not exempt a covered entity from liability under common law,” it is inherently inconsistent with the language of Section 6(a), which prohibits a State from enforcing any “rule . . . duty, requirement, [or] standard . . . having the force and effect of law,” a phrase that appears to refer to and encompass common law. Bill, §6 (a), (b).

² See Mass. Gen. Law ch. 266, § 120F (“Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both. The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.”).

laws meant to protect medical records and mental health records from unauthorized access (*see, e.g.,* Mass Gen. Law ch. 111, § 70E(b), and ch. 123, § 36). Indeed, Section 6(a) could even be read to divest enforcement authority specifically given to the States under other federal laws relating to data security, including, for example, the “Security Standards for the Protection of Electronic Protected Health Information” (45 C.F.R. Subpart C of Part 164), which are enforceable by the States under the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 1320d–5(d)).

Finally, by prohibiting a State from “adopt[ing] ... any law ... [or] regulation ... relating to or with respect to the security of data in electronic form,” Section 6(a) would have a chilling effect on innovation and adaption by state legislatures and policy-makers in responding to data security and privacy threats. New laws or regulations to prevent or penalize identity theft or that address security concerns that arise from future technologies, for example, could arguably be subject to a preemption challenge under Section 6(a) because they “relate to the security of data in electronic form.” Legislative agility and regulatory rule-making is especially important in the field of data security, where new technologies and changing notions of privacy and security may raise data security risks impossible to foresee or which cannot be addressed by this Bill. Section 6(a) essentially “freezes” data security and breach notification standards in time without regard to future, unforeseen risks.

2. How is the breadth of the preemption language in Sections 6(a) and 6(b) of the discussion draft harmful to consumers?

Articulated, minimum data security standards are imperative to safeguard the privacy and security of consumers’ personal information. It is equally important that such standards be flexible and responsive to changing risks and technologies. The Bill, however, divests the States of their authority to establish or enforce any existing data security laws or regulations (*e.g.* 201 CMR 17.00), and imposes in their place the requirement that a covered entity “implement and maintain reasonable security measures and practices.” Bill, § 2. As we have previously stated, in the absence of specifically defined regulatory guidance (*e.g.,* from the Federal Trade Commission (“FTC”)), this amorphous standard is too vague to achieve the Bill’s stated goal of “protect[ing] consumers from identity theft, economic loss or economic harm, and financial fraud.” Bill, § 1(b).

Data breaches are an ever-present and increasing threat for companies of all sizes and from all industries. Massachusetts’ experience enforcing its data security regulations (201 CMR 17.00) shows that while some breaches reported to this Office in 2014 appear to have resulted from intentional, criminal acts, many resulted from the improper disposal of consumers’ information, lost files, disclosure through inadvertence, carelessness, or the failure to follow basic and well-accepted data security practices and procedures. Our enforcement experience suggests even those data breaches resulting from intentional criminal attacks could have been

³ *See* Mass. Gen. Law ch. 272, § 99(C) (“any person who— willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment”).

avoided or mitigated if the entity had complied with its own data security policies or employed basic security practices such as software updates or firewalls. In an era of rising data breach risks,⁴ the need for strong and enforceable minimum data security standards is imperative.

Unfortunately, the data security standard set forth in Section 2 of the Bill is weaker than the state laws (including Massachusetts') the Bill would preempt, and as measured against other federal regimes.⁵ Specifically, because the Bill fails to define or enumerate any of the required "reasonable security measures and practices," or provide any regulatory agency with rule-making authority to do so, it would force covered entities to guess what constitutes such "reasonable security measures and practices," risking a downward harmonization towards the least expensive (and likely least effective) measures and practices. The resulting litigation to establish data security standards by judicial interpretation will not keep pace with evolving technology and security threats, and will expose consumers' sensitive personal information to unnecessary risk.

Finally, because Section 6 does not provide for recovery of consumer restitution, and because Section 4(c) prohibits a private right of action by a consumer, a consumer would not be able to seek compensation for the financial consequences of a data breach. This prohibition, together with the inability of a state Attorney General to recover restitution for injured consumers under the Bill, will result in victimized consumers effectively being left without remedy. Such an outcome is directly contrary to the stated purpose of the Bill to "protect consumers from identity theft, economic loss or economic harm, and financial fraud." Bill, § 1(b).

3. How are the enforcement powers conferred to the state Attorneys General under Section 4(b) of the Discussion Draft insufficient to maintain even current levels of state enforcement?

Although Section 4(b) of the Bill grants enforcement authority to the States, various other provisions of the proposed Bill undercut the States' ability to effectively exercise it. Most significantly, the Bill does not require notice of a security breach to any regulator – state or federal – in the event fewer than 10,000 consumers are affected and, then, only requires notice to

⁴ Since September 1, 2007, through December 31, 2014, this Office has received notice of over 9,800 breaches, reporting over 5 million impacted Massachusetts residents, with 2,409 breaches reported in 2014 alone (a 33% increase over 2012, and over a 527% increase over 2008).

⁵ Similar to existing federal standards applicable to financial institutions (see 16 C.F.R. Part 314 ((Standards for Safeguarding Customer Information)) and entities covered under HIPAA (see e.g. 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information)), Massachusetts requires entities to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information (201 CMR 17.03(2)(b)); develop, implement and maintain a "written comprehensive information security program" containing physical, administrative and technical safeguards necessary to protect personal information from those risks (201 CMR 17.03); take reasonable steps to oversee third parties handling personal information (201 CMR 17.03(2)(f)); and securely dispose of personal information (Mass Gen. Law ch. 93I). Cognizant of the particular risks associated with electronic data, Massachusetts also requires entities, among other things, to establish and maintain a technically-feasible computer security system (201 CMR 17.04); and to encrypt personal information sent over public networks or wirelessly, or stored on laptops and portable devices (201 CMR 17.04(3), (5)).

the FTC. Bill, § 3(a)(3). Currently under the Massachusetts Data Breach Notification Act (Mass. Gen. Law ch. 93H), this Office must receive notice of any data breach impacting one or more Massachusetts residents. These notices provide this Office with essential insight into emerging data security threats and enable this Office to ensure that consumers are promptly and appropriately notified.⁶ Under the Bill, this Office would receive no notices – even when a breach impacts a significant number of Massachusetts residents, or only Massachusetts residents. Even if the FTC were to share with the States the notices it receives under the Bill, a threshold of 10,000 consumers is too high to enable the States to effectively protect its residents.⁷ As a result, the Bill would create a significant enforcement “blind spot” to smaller-scale breaches, even where the breaches resulted from unreasonable data security practices and where consumers remain subject to unnecessary and avoidable risks.

Other provisions of Section 4(b) would unnecessarily complicate and burden the States’ efforts to enforce the requirements of the Bill. A State would have to bring an enforcement action in federal court, provide prior notice to the FTC, and abstain in the event the FTC initiated an action first. Such limits subject each State to unnecessary expense and potential delay while consumers’ personal information potentially remains at risk. Additionally, Section 4(b) restricts the remedies a State may pursue, capping civil penalties at \$2,500,000 per event⁸ without regard to the extent of consumer harm, and preventing the State from seeking restitution on behalf of injured consumers. These significant obstacles, coupled with Section 4(c)’s explicit prohibition of any private right of action, will not only impede state enforcement but also leave consumers without any meaningful remedy or protection in the event their personal information is compromised by a breach of security.

* * *

We appreciate this opportunity to convey to the Subcommittee our serious concerns regarding the effectiveness of the Bill to meet its intended purpose to protect consumers from data security breaches. As you can see, where the Bill may have intended to set a common floor of national consumer protections, it also sets a ceiling in States where laws currently provide greater consumer protections than the Bill would provide. Please do not hesitate to contact us for additional detail or clarity, or with questions you may have. We are happy to provide you with

⁶ While this Office investigates only a small fraction of the data breaches about which it receives notice, those notices also allow this Office to effectively monitor to ensure that consumers’ personal information is appropriately protected from breach.

⁷ In Massachusetts, fewer than 3% of the breaches reported in 2013 met that threshold. Each of those breaches impacted, on average, 74 Massachusetts residents.

⁸ As this Office previously stated, this cap may be an insufficient deterrent, and could be treated as cost of doing business. In light of even limited history, this figure is too low and would constitute Congress’ encouraging businesses to underinvest in consumer protections. Prior data security settlements have involved much higher monetary penalties, including the \$9.75 million monetary payment by the TJX Companies to settle a 41-state multistate investigation regarding a 2007 data breach that put the personal information of over 45 million consumers at risk. See *In re: The TJX Companies, Inc.*, Case No. 09-2602 (Mass. Sup. Ct. June 28, 2009).

any information you may need or to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws.

Sincerely,

A black rectangular redaction box covering the signature of Jonathan B. Miller.

Jonathan B. Miller
Chief, Public Protection and Advocacy Bureau

Sara Cable
Assistant Attorney General
Consumer Protection Division

Office of Attorney General Maura Healey
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108
(617) 727-2200

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) 225-2327
Minority (202) 225-3641

July 13, 2015

Mr. Mallory Duncan
Senior Vice President
National Retail Federation
1101 New York Avenue, N.W.
Washington, D.C. 20005

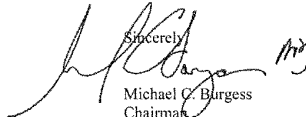
Dear Mr. Duncan,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015."

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 with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

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

[Mr. Duncan did not answer submitted questions for the record by the time of printing.]

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 (201) 225-2077
Minority (202) 225-3641

July 13, 2015

Ms. Laura Moy
Senior Policy Counsel
Open Technology Institute
New America
1899 L Street, N.W. Suite 400
Washington, D.C. 20036

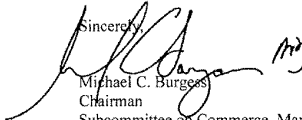
Dear Ms. Moy,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015."

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 with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

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

[Ms. Moy's answers to submitted questions for the record have been retained in committee files and also are available at <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf>.]

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

July 13, 2015

Ms. Yael Weinman
Vice President
Global Privacy and General Counsel
Information Technology Industry Council
1101 K Street, N.W. Suite 610
Washington, D.C. 20005

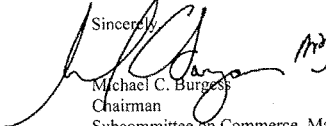
Dear Ms. Weinman,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015."

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 with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

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



Information Technology Industry Council

Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

March 18, 2015 Hearing

"Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015"

Responses of Ms. Yael Weinman, VP, Global Privacy Policy and General Counsel
Information Technology Industry Council (ITI)

Written Questions for the Record from the Honorable Michael C. Burgess to Yael Weinman

1. We have heard a lot about the issues companies face complying with 47 different State data breach notification laws. How would your member companies navigate complying with 47 different State data security requirements? Does that change if the States include specific technical or process requirements?

Navigating differing data security requirements would pose significant challenges, particularly if they included specific technical or process requirements. Different requirements could be conflicting and specific technical or process requirements could in fact lower the level of security in that they would mandate specific requirements rather than permitting entities to innovate and provide a greater level of security than that which might be specified in the letter of the law.

2. Why is the draft bill's preemption of existing State laws important for both consumers and businesses?

For businesses, preemption is important because it would streamline the notification process, enabling businesses to provide notices more consistently and efficiently, freeing up resources to address the numerous tasks that must be undertaken when a data breach occurs. Consistent notices would reduce confusion for businesses—particularly smaller businesses—as to how and when to notify their customers who reside in different states, each requiring a different type of or content for notification and under differing circumstances.

For consumers, preemption would ensure consistent notices across states and jurisdictions thereby reducing consumer confusion that may result from the variances of the method of data breach notifications, the content of such notifications, and the circumstances of such notification. Reducing consumer confusion is paramount in ensuring that consumers take appropriate action upon notification of a data breach.

Information Technology Industry Council
1101 K St. NW Suite 610, Washington, D.C. 20005
T +1 (202) 737-8888, www.iti.org

Innovation. Insight. Influence.