

**LEGISLATIVE PROPOSALS TO REFORM
THE CURRENT DATA SECURITY AND
BREACH NOTIFICATION REGULATORY REGIME**

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

—————
MARCH 7, 2018
—————

Printed for the use of the Committee on Financial Services

Serial No. 115-78



—————
U.S. GOVERNMENT PUBLISHING OFFICE

31-383 PDF

WASHINGTON : 2018

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
PETER T. KING, New York	CAROLYN B. MALONEY, New York
EDWARD R. ROYCE, California	NYDIA M. VELÁZQUEZ, New York
FRANK D. LUCAS, Oklahoma	BRAD SHERMAN, California
STEVAN PEARCE, New Mexico	GREGORY W. MEEKS, New York
BILL POSEY, Florida	MICHAEL E. CAPUANO, Massachusetts
BLAINE LUETKEMEYER, Missouri	WM. LACY CLAY, Missouri
BILL HUIZENGA, Michigan	STEPHEN F. LYNCH, Massachusetts
SEAN P. DUFFY, Wisconsin	DAVID SCOTT, Georgia
STEVE STIVERS, Ohio	AL GREEN, Texas
RANDY HULTGREN, Illinois	EMANUEL CLEAVER, Missouri
DENNIS A. ROSS, Florida	GWEN MOORE, Wisconsin
ROBERT PITTENGER, North Carolina	KEITH ELLISON, Minnesota
ANN WAGNER, Missouri	ED PERLMUTTER, Colorado
ANDY BARR, Kentucky	JAMES A. HIMES, Connecticut
KEITH J. ROTHFUS, Pennsylvania	BILL FOSTER, Illinois
LUKE MESSER, Indiana	DANIEL T. KILDEE, Michigan
SCOTT TIPTON, Colorado	JOHN K. DELANEY, Maryland
ROGER WILLIAMS, Texas	KYRSTEN SINEMA, Arizona
BRUCE POLIQUIN, Maine	JOYCE BEATTY, Ohio
MIA LOVE, Utah	DENNY HECK, Washington
FRENCH HILL, Arkansas	JUAN VARGAS, California
TOM EMMER, Minnesota	JOSH GOTTHEIMER, New Jersey
LEE M. ZELDIN, New York	VICENTE GONZALEZ, Texas
DAVID A. TROTT, Michigan	CHARLIE CRIST, Florida
BARRY LOUDERMILK, Georgia	RUBEN KIHUEN, Nevada
ALEXANDER X. MOONEY, West Virginia	
THOMAS MACARTHUR, New Jersey	
WARREN DAVIDSON, Ohio	
TED BUDD, North Carolina	
DAVID KUSTOFF, Tennessee	
CLAUDIA TENNEY, New York	
TREY HOLLINGSWORTH, Indiana	

SHANNON MCGAHN, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

BLAINE LUETKEMEYER, Missouri, *Chairman*

KEITH J. ROTHFUS, Pennsylvania, *Vice
Chairman*

EDWARD R. ROYCE, California

FRANK D. LUCAS, Oklahoma

BILL POSEY, Florida

DENNIS A. ROSS, Florida

ROBERT PITTENGER, North Carolina

ANDY BARR, Kentucky

SCOTT TIPTON, Colorado

ROGER WILLIAMS, Texas

MIA LOVE, Utah

DAVID A. TROTT, Michigan

BARRY LOUDERMILK, Georgia

DAVID KUSTOFF, Tennessee

CLAUDIA TENNEY, New York

WM. LACY CLAY, Missouri, *Ranking
Member*

CAROLYN B. MALONEY, New York

GREGORY W. MEEKS, New York

DAVID SCOTT, Georgia

NYDIA M. VELAZQUEZ, New York

AL GREEN, Texas

KEITH ELLISON, Minnesota

MICHAEL E. CAPUANO, Massachusetts

DENNY HECK, Washington

GWEN MOORE, Wisconsin

CHARLIE CRIST, Florida

CONTENTS

	Page
Hearing held on:	
March 7, 2018	1
Appendix:	
March 7, 2018	37

WITNESSES

WEDNESDAY, MARCH 7, 2018

Cable, Sara, Director, Data Privacy and Security, and Assistant Attorney General, Office of the Attorney General, Commonwealth of Massachusetts ..	3
Creighton, Francis, President and Chief Executive Officer, Consumer Data Industry Association	5
Kratovil, Jason, Vice President, Financial Services Roundtable	9
Miller, John S., Vice President, Global Policy and Law, Information Technology Industry Council	7

APPENDIX

Prepared statements:	
Cable, Sara	38
Creighton, Francis	100
Kratovil, Jason	126
Miller, John S.	151

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Luetkemeyer, Hon. Blaine:	
Written statement from American Bankers Association (ABA)	167
Written statement from Consumer Bankers Association (CBA)	180
Written statement from Center for Democracy & Technology (CDT)	182
Coalition letter dated March 7, 2018	184
Written statement from Credit Union National Association (CUNA)	187
Written statement from Independent Community Bankers of America (ICBA)	189
Written statement from National Association of Convenience Stores (NACS)	191
Written statement from National Association of Federally-Insured Credit Unions (NAFCU)	193
Written statement from National Retail Federation (NRF)	196
Letter from Kathleen McGee, State of New York Office of the Attorney General	227
Letter from Rapid7	233
Letter from Society of Independent Gasoline Marketers of America (SIGMA)	236
Green, Hon. Al:	
Written statement from American Council of Life Insurers (ACLI)	238
Financial trades letter dated February 28, 2018	241
Written statement from Property Casualty Insurers Association of America (PCI)	243
Retailer coalition letter dated February 13, 2018	246
Cable, Sara:	
Written responses to questions for the record submitted by Representatives Waters and Ross	250

VI

	Page
Creighton, Francis:	
Written responses to questions for the record submitted by Representatives Waters and Ross	263
Kratovil, Jason:	
Written responses to questions for the record submitted by Representatives Waters and Ross	275
Miller, John S.:	
Written responses to questions for the record submitted by Representatives Waters and Ross	283

**LEGISLATIVE PROPOSALS TO REFORM
THE CURRENT DATA SECURITY AND BREACH
NOTIFICATION REGULATORY REGIME**

Wednesday, March 7, 2018

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

The subcommittee met, pursuant to notice, at 2:01 p.m., in room 2128, Rayburn House Office Building, Hon. Blaine Luetkemeyer [chairman of the subcommittee] presiding.

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

Also present: Representative Hensarling.

Chairman LUETKEMEYER. The committee will come to order. Without objection, the Chair is authorized to declare recess of the committee at any time.

This hearing is entitled, "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime." Before we begin, I would like to thank the witnesses for appearing today. We appreciate your participation and look forward to the discussion.

We have a great crowd today. We must have a very, very interesting subject. So, thank you all for being here.

I now recognize myself for 5 minutes for purposes of doing an opening statement. Forty-eight States, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have all enacted differing laws requiring private companies to notify individuals of breaches of personal information. For each State with robust safeguards or requirements in place, there is another with protections that are simply insufficient, creating a labyrinth that causes compliance nightmares while leaving uncertainty or certainty as needed the most, consumer notification.

And although these laws only cover certain sectors, the protections vary widely from State to State. It is important to ensure all consumers are afforded better protections and more prompt notifications. Look at my home State of Missouri, where our two largest cities straddle State borders. There is no reason why a consumer sitting in East Saint Louis, Illinois should have greater protections than one sitting less than 10 minutes away in Saint Louis.

One individual's personal information is no more or less valuable than another's. This is a national problem that requires an immediate national solution, which is my legislation developed with the gentlelady from New York, Mrs. Maloney, is both timely and necessary. First and foremost, our legislation would create a national security standard for entities that access, maintain, store, or handle personal information, while providing flexibility based on an individual company's size, complexity, and sensitivity of the information it maintains.

With a responsible Federal standard in place, companies will no longer have to spend valuable time tracking a maze of regulations. That time can be better spent actually securing the personal information of their customers and innovating to fight against cyber crime. The draft legislation also includes robust law enforcement and consumer notification regimes. A covered entity has the responsibility to conduct an immediate investigation and take responsible measures to restore the compromised system.

If it is determined that the breach has or will cause identity theft, fraud, or economic loss, the breached entity must notify immediately law enforcement. On the consumer side, the bill requires immediate notification without unreasonable delay to any consumer who may be impacted by a breach of his or her personal information. This is a strict timeline that rivals even the most aggressive State laws. After all, it is the consumer that should be front and center in any conversation surrounding the protection of data.

Today, we will also examine legislation introduced by the gentleman from North Carolina, Mr. McHenry. His PROTECT Act would establish a new regulatory regime for credit reporting agencies. Mr. McHenry's work on this legislation and on the broader issue of data security and the protection of consumer information has been an integral part of this debate, and we all appreciate his leadership.

This isn't a question of if, but when there will be another data security breach and the personal information of too many consumers will be compromised. Congress will move a product across the finish line. The legislation we consider today aims to foster an environment where consumers are not just protected but empowered. This is a challenging issue, one that has been seriously debated in Congress for well over a decade, and the time to act has come.

It is essential that the industry looks at the bigger picture here and realizes the immeasurable benefits data security safeguards and responsible notification process will have on their customers and businesses. While some of us may experience short-term pain, it will be far outweighed by the long-term gain of delivering meaningful results for the American people.

I thank my friend from New York, Mrs. Maloney, for working with me on this discussion draft and the gentleman from North Carolina for his diligent work on his legislation as well.

We have an excellent panel of witnesses today. I want to thank you for appearing. I look forward to your testimony. The Chair now recognizes the gentleman from Missouri, Mr. Clay, the Ranking

Member of the subcommittee for 5 minutes for an opening statement.

Mr. CLAY. Thank you, Mr. Chairman. I certainly will not take the total 5 minutes. But I want to thank you for holding this hearing.

Breaches are a growing problem and credit reporting agency Equifax just reported one of the largest breaches ever. On July 29, 2017, Equifax detects their security breach. Bloomberg reported that regulatory filings showed that on August 1st, Chief Financial Officer John Gamble sold shares worth \$946,000 and Joseph Loughran, President of U.S. Information Solutions exercised options to dispose of stock worth \$584,000. Rodolfo Ploder, President of Workforce Solutions, sold \$250,000 worth of stock on August 2nd. None of the filings list the transactions as being part of 10b5-1 scheduled trading plan.

On September 7, 2018, Equifax officially announces the security breach to the public. The company directs consumers to a dedicated website to check if they are included in the breach. October 2, 2017, Equifax announces that forensic computer security company Mandiant has identified another 2.5 million people whose personally identifiable information has been compromised, taking the number of victims from 143 million to 145.5 million. On March 1, 2018, Equifax reported that another 2.4 million Americans were impacted by their already enormous data breach. That brings the total to 147.9 million Americans.

We can all agree that consumers in the United States face a data protection crisis. Currently, no Federal law requires credit reporting agencies to offer credit freezes. So, I look forward to this discussion and working with the Chairman and others on this legislation.

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

Chairman LUETKEMEYER. The gentleman yields back.

Today, we welcome the testimony of Ms. Sara Cable, Director for Data Privacy and Security and Assistant Attorney General of the Commonwealth of Massachusetts; Mr. Francis Creighton, President and CEO, Consumer Data Industry Association (CDIA); Mr. John Miller, Vice President, Global Policy and Law, Information Technology Industry Council (ITI); and Mr. Jason Kratovil, Vice President, Financial Services Roundtable (FSR).

We certainly thank each of you for being here today and just a quick tutorial on those of you who haven't been here before on the microphone system, please turn it on when you get ready to speak. The green light will show and when you are getting ready to the 1-minute mark left to talk, you get five to speak, it will be yellow. And whenever you get that all done it is red, and about that time I start to raise my gavel. So, we will get along real well today. I am sure.

With that, we want to start with Ms. Cable. Welcome, and you are recognized for 5 minutes.

STATEMENT OF SARA CABLE

Ms. CABLE. Thank you, Chairman Luetkemeyer, Ranking Member Clay, distinguished members of the subcommittee. I appreciate being here today.

My name is Sara Cable. I am an Assistant Attorney General with the Massachusetts Attorney General's Office and I am the Director of Data Privacy and Security for its Consumer Protection Division. I am here today on behalf of my office to testify as to our concerns with the discussion draft bill, the Data Acquisition and Technology Accountability and Security Act.

My comments today are informed by my office's over a decade's worth of experience in enforcing the Massachusetts data breach notice law and data security regulations, which are regarded as among the strongest in the country. This office works hard to use those laws to protect our consumers and we think that our consumers are better off as a result.

We are encouraged that the subcommittee recognizes the critical necessity of data security and breach protections for consumers, and we share this goal. The constant drum beat of breaches over the last few years affecting some of the largest and most sophisticated companies has brought the issue of data insecurity to the forefront of the public's consciousness. It is clear that more must be done to protect consumers and preserve confidence in the marketplace.

Now is not the time to dilute the tools regularly and successfully used by many States including Massachusetts to combat this crisis. The subcommittee's first priority should be on enhancing the existing protections consumers have under State law, not minimizing compliance cost for businesses that allow these breaches to occur.

While we understand that Federal standardization is the thrust of the bill, Congress should not expose American consumers to increased risks as a result of a new, less stringent national standard. In our view, this bill would harm, not help, consumers. It would restrict, not protect or even preserve, the existing authority and role of the State AGs (attorneys general) and it would disregard, not respect, the important role of the States to enact protections they deem appropriate for their own consumers.

I want to make my first point concerning the bill's consumer notice provisions. Our view is that the notification provision as drafted will leave consumers in a worse position than the status quo. If preventing consumer harm is the goal of a data breach notice regime which we think it is, quickly notifying consumers that their data has been compromised must be the first priority. This allows that consumer time to take steps to protect their identity before the hacker or an identity thief uses the breached information against them.

The consumer notice standards in this bill, as found in section 4b-2, do not protect the consumers. They require notice only after the consumer has suffered harm. This is contrary to today's regime where consumers under most State laws are notified of breaches before the harm occurs. Notifying consumers of the breach after they are already harmed does little for the consumer and instead, it allows entities to pass the costs of its poor data security on to consumers and this is unacceptable in our view. Especially unfair because the bill does not clearly authorize any mechanism to remedy this harm, including by not giving clear authority to the State attorneys general to obtain restitution or consumer damages.

My second point concerns the proposed enforcement mechanisms of the bill which make it harder for our office to protect our consumers. The State AGs are the cops on the beat. We have been on the frontlines of this problem for over a decade. We use our authority under our consumer protection laws and personal information protection acts to protect our consumers from breaches and hold companies accountable for failing to protect that data. This bill makes it harder for us to do our jobs.

Among other problems that I have laid out in my written testimony, the bill does not require entities to notify State AGs of breaches impacting their State's residents. Under Massachusetts law and currently under the law of at least 24 other States, State AGs get direct notice of breaches impacting their residents, and this notice is critical for us because it allows us to understand whether our consumers are impacted and gives us an informed and comprehensive view of the risks that are out there for consumers.

Over the last decade, 21,000 data breaches have been reported to the Massachusetts Attorney General's Office. There were 3,800 reported last year and as currently drafted, we would get notified of none of these breaches. We also want to point out that the threshold for Federal notice of 5,000 individuals affected we believe is too high and will fail to capture breaches that have a significant impact in a State.

For example, in Massachusetts, less than 1 percent of the 3,800 breaches last year met this criteria and indeed 93 percent of the 3,800 breaches impacted fewer than 100 residents each. So, we think this bill would create a significant blind spot for Federal or State enforcement of poor security practices by businesses. Thank you.

[The prepared statement of Ms. Cable can be found on page 38 of the Appendix.]

Chairman LUETKEMEYER. OK. Thank you for your testimony.

Mr. Creighton, you are recognized for 5 minutes.

STATEMENT OF FRANCIS CREIGHTON

Mr. CREIGHTON. Thank you.

Before discussing the legislation before us today and how it would impact CDIA members and the credit reporting system in general, I would like to just give a brief context about how credit bureaus help the economy and how we are already regulated.

Our credit reporting system today is the envy of the world. It is a main reason we have such a diverse range of lenders and products from which to choose. Without it, without access to a full consumer report, community banks, credit unions, insurance companies, and others won't know how a consumer has handled their obligations unless they already know the customer. Without credit reporting, smaller institutions would not be able to compete against the very largest banks for your business.

Credit reports are a check on human bias and assumptions by providing facts that contribute to equitable treatment. CDIA members make possible an accountable and color-blind system. Without it, subjective judgments could replace the facts of creditworthiness. Credit reporting companies are also innovating to solve the problem of the un-banked, thin file, and credit-invisible consumers who

have not had a chance to participate in the mainstream financial system, a goal shared by many on this committee.

The Federal Fair Credit Reporting Act (FCRA) which governs credit reporting subjects credit reporting companies to a comprehensive regulatory and consumer protection regime. The FCRA protects privacy. It includes criminal penalties for people who abuse the system, mandates the accuracy and completeness of consumer reports and makes the process transparent for consumers. On data security, under the Gramm-Leach-Bliley Act (GLBA), the nationwide consumer reporting agencies are subject to the FTC's (Federal Trade Commission's) Safeguards Rule as non-bank financial institutions. We are also regulated and face enforcement in current law by the States.

Contractual obligations from our financial institution customers make sure we meet the requirements of the Federal Financial Institutions Examinations Council (FFIEC). At every level, this is a well regulated industry. The PROTECT Act, one of the bills before us today, would establish a new FFIEC data security regulator for our companies. We believe that any major change like this would be better informed by the outcome of the Equifax investigation, which is still ongoing by the FTC and the CFPB (Consumer Financial Protection Bureau).

The PROTECT Act also establishes a uniform standard for credit freezes. We believe that this is in the best interest of consumers who share the same concerns whether they live in Missouri or Massachusetts. The patchwork quilt of State laws creates confusion. Every consumer should have the same right regardless of where they live. The last major provision of the PROTECT Act would be to eliminate the use of Social Security numbers in 2 years. We do not believe that this is a feasible proposal and we look forward to working with Mr. McHenry and this subcommittee on alternatives and marketplace innovations.

We have obligations under the FCRA to ensure maximum possible accuracy, and the SSN is critical to meeting that legal obligation. We use SSNs for the same reasons that Government does. They are the only reliable and universal identifier. SSNs help ensure that information is matched with the correct file. There simply is no other identifier currently in existence that gives us the confidence required to meet our statutory obligations.

We take our data security responsibility seriously, especially in light of the breach at Equifax. While the investigation there is not yet completed as I said, it has put a spotlight on our companies. We know that the most important thing is not how a company responds to a breach; it is preventing the breach in the first place. The Chairman's legislation establishes a national standard for both data security and for breach notification. The bill's provisions would allow a company's prudential regulator to enforce these rules, setting up the FTC as the regulator for those without one already, with enforcement by State attorneys general.

Since credit bureaus are financial entities under GLBA, they would continue to be subject to the FTC's Safeguards Rule and to civil penalty authority for violations of the breach notification provision of the bill. The trigger for what constitutes a data breach is

well defined, reasonable risk that the breach of data security has resulted in identity theft, fraud, or economic loss.

We are pleased to note that for breaches over 5,000 consumers, credit bureaus can be notified ahead of others, ensuring that we can prepare for the increased volume that a large breach generates. This legislation broadly conforms to the policy goals CDIA members have had for breach notification legislation and we are pleased to note the different interests who are working together to solve this problem. As the legislative process moves forward on both of these bills, we anticipate that there will be perfecting amendments to improve them, and we look forward to working with the bills' sponsors and other members of the committee on whether and how to reform our data security and breach notification regulatory regimes.

I look forward to your questions. Thank you.

[The prepared statement of Mr. Creighton can be found on page 100 of the Appendix.]

Chairman LUETKEMEYER. Thank you, Mr. Creighton.

Mr. Miller, you are recognized for 5 minutes.

STATEMENT OF JOHN MILLER

Mr. MILLER. Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, on behalf of ITI and its member companies, thank you for the opportunity to testify today on the discussion draft of the Data Acquisition and Technology Accountability and Security Act.

ITI is a global policy and advocacy organization representing over 60 of the world's leading information and communications technology companies from all corners of the sector, including hardware, software, Internet, networking, and services companies. Our members are not only technology solutions providers, but are also stewards of their own sensitive data. As such, we have interests as both covered entities and third parties in advancing Federal data security and data breach notification legislation that serves important consumer protection interests.

Chairman Luetkemeyer and Congresswoman Maloney, I would like to begin my remarks by commending you for the transparent and inclusive process through which you and your staffs have worked to develop the discussion draft. We share your goal of developing a uniform consumer protective data security and breach regime and appreciate the openness with which you have considered our priority issues. Congress and the business community have worked for more than a dozen years to develop a regime that balances the concerns of all stakeholders, and this effort moves us closer to realizing that shared goal.

We recognize that compromises must be made to move this effort forward and we do not wish the perfect to be the enemy of the good. In that spirit of compromise, ITI supports many of the provisions in the discussion draft but we also offer several recommendations aimed at further improving and clarifying the draft language. ITI developed principles that a data breach law must include to achieve much needed regulatory clarity and certainty. We are pleased the discussion draft reflects the majority of these principles by preempting the existing patchwork of State laws to reduce con-

sumer confusion and ensure quicker and more consistent notifications, providing an exception for information that is rendered harmless via technology such as encryption; avoiding over-notification by appropriately limiting the definition of personal information to data that can be used to inflict concrete financial harms; acknowledging consumers are not well served by receiving notices from companies they do not recognize, but allowing companies and their third-party vendors to agree on notification responsibility by contract as appropriate; and recognizing criminal penalties are inappropriate for companies who are themselves victims of criminal hacks.

Regarding the security provisions in the bill, ITI has long advocated for security approaches that are voluntary, grounded in sound risk management principles and international standards, foster innovation in cybersecurity and data protection, and are scalable for organizations of all sizes and sophistication. Flexibility is key, as a company must be able to protect the information it holds in a manner that is reasonable and appropriate to the nature of its business resources and the sensitivity of the data it handles.

The security safeguards appear largely consistent with these key security principles, but we are concerned about the multilayered approach established by the bill which sets forth an enumerated list of sometimes prescriptive safeguards layered by a reasonable security standard. To help alleviate this concern, we recommend the inclusion of a heightened burden of proof for regulators, which would simply require a more thorough showing that a company who relied on and complied with the Government-directed safeguards and yet still suffered a breach nevertheless lacked reasonable security.

In addition to this suggestion, my written testimony offers several additional recommendations to improve and clarify the proposed notification regime. I will briefly highlight a few of these recommendations here.

First, the discussion draft requires notification be made immediately and without unreasonable delay. There are several reasons why immediate notification is not only infeasible but often inadvisable. Chief among them is that consumers will be subject to further harm by would-be thieves if the public is alerted to security vulnerabilities prior to their remediation. We recognize the urgency required in notification and recommend utilizing existing language from one of the existing State laws to more effectively balance these considerations.

Second, the discussion draft requires third parties to notify covered entities if breached personal data has or may have occurred. Our companies deal with a large volume of security incidents daily, and while breaches are frequently suspected, preliminary investigations often reveal no breach occurred. Third parties cannot and should not be expected to notify based on a guess as to whether a breach may have happened. They must be afforded the same opportunity as covered entities to conduct an investigation to determine whether the security incident resulted in a compromise of data.

Third, as the definitions are drafted, third parties will simultaneously be considered covered entities in most instances. This is problematic, because the discussion draft imposes different require-

ments on covered entities versus third parties. So, the overlapping definitions will subject third parties to divergent sets of requirements for the same activity. The definition of “covered entity” must be amended to focus on entities that own or license the data.

Fourth, the discussion draft permits unlimited civil penalties arising from a single incident. Most data breaches are the result of criminal acts. Organizations can and should do their part to protect consumer data from unauthorized access and acquisition, but uncapped civil penalties are seemingly punitive in nature and not appropriate when an organization has been victimized by criminals or a nation state.

Thank you again for the opportunity to share our perspective here today. I look forward to your questions.

[The prepared statement of Mr. Miller can be found on page 151 of the Appendix.]

Chairman LUETKEMEYER. Mr. Miller, thank you so much.

Mr. Kratovil, you are recognized for 5 minutes. You have a very high bar to keep. Each one of these witnesses so far has stayed right at underneath their 5-minute allotment here.

STATEMENT OF JASON KRATOVIL

Mr. KRATOVIL. Mr. Chairman, Ranking Member Clay, and members of the subcommittee, on behalf of the leading banking and payments members of FSR, thank you for having me here today to discuss two proposals closely linked in their goals to improve cybersecurity and the protection of consumers’ credit.

For companies across the economy, data isn’t just a nice thing to have. It is increasingly the engine of modern commerce. For the better part of 13 years, I have been involved in this committee’s work on data security legislation. Back in 2005 when I worked for the late Congressman Steve LaTourette, this committee passed his bipartisan legislation, marking the first time a Congressional committee directly tackled this issue.

Back then, high-profile data breaches grabbed headlines much as they do today, but it was in many ways a simpler time. The ability to harness the power of data was confined to the Government or the largest, most sophisticated companies. Household budgeting relied on balancing a checkbook, not data aggregation platforms running advanced APIs, and the cloud was simply an object in the sky.

While times have certainly changed, some principles remain the same. Over the last 13 years, the financial industry has consistently called for Congress to enact data security legislation that sets strong but flexible and scalable requirements for companies across the economy to protect data and to ensure consumers receive notice of a breach when they are at risk. The proliferation of sensitive consumer data across the economy has only heightened the need for Congress to act.

Today, a business with only a few employees and modest resources can obtain the technology or develop an app to allow them to come into contact with millions of pieces of data. The implications of this from a consumer privacy and business ethics perspective are significant. The discussion for policymakers, however, must begin with security. That is why both the PROTECT Act offered by Congressman McHenry and Mr. Chairman, the discussion draft of

data security and breach notice legislation you and Congresswoman Maloney have put forward are both so important and timely.

The discussion draft of data security legislation is an excellent start and represents the best opportunity I have seen to actually get a bill through the House. I provide a more detailed review of both proposals in my written testimony, but would like to offer a few observations on the Chairman's discussion draft.

First, your draft sets a high bar for data security. For the financial sector, this is critical. Underlying our advocacy for Federal legislation is the hope that with the right standard, the number of incidents can actually be reduced. Reaching the right threshold means spelling out a process and risk-based framework for companies to follow. Federal legislation should not expect the small mom-and-pop merchant to deploy the same cyber resources as their larger counterparts. Your draft sets the right standard while not unduly burdening firms that have little or no exposure to sensitive data.

Second, we strongly believe notification to consumers must be tied to an assessment of risk as the discussion draft makes clear. By that, a breach of commonly available phonebook-type information or sensitive information that is encrypted should not trigger notice. Notice must be viewed by consumers as a call to action, based on an assessment that the nature of a breach has exposed them to a risk of financial fraud.

Over-notification makes us desensitized. I guess most of us are guilty of throwing out yet another breach letter we received in the mail. With this draft, Congress has an opportunity to reframe the importance of breach notification, making receipt of a notice something we as consumers take seriously.

Third, the United States has favored a sectoral approach to the regulation of data security and that approach should be preserved. By that, I mean new legislation should recognize that sectors including the financial industry have existing Federal obligations to secure data and notify consumers of a breach and not add duplicative responsibilities.

Finally, we believe preemption of the patchwork of State laws is the right approach for Congress to take. Few issues better illustrate the need for a uniform Federal standard as data breach. That said, I would be very concerned if the measure before us only amounted to a weak data protection standard. However, as I mentioned, the discussion draft hits the right mark.

In conclusion, with the lessons of history as our guide, it is clear that finding consensus is critical if we want to see data security legislation enacted. FSR has worked for many years to help bridge the policy divides that have caused the legislative process to stall in the past. As evidenced by this panel, more stakeholders are at the table today than ever before, ready to work with this committee and others in the interest of seeing a strong piece of consumer protection legislation signed into law.

Thank you, Mr. Chairman. I look forward to your questions.

[The prepared statement of Mr. Kratovil can be found on page 126 of the Appendix.]

Chairman LUETKEMEYER. Thank you, Mr. Kratovil, and I thank all of our witnesses. You guys did a great job and we certainly appreciate your thoughtful suggestions. And again, we are discussing a draft legislation with regards to what we are doing with our particular bill. And so, it is a work in progress and we appreciate your willingness to work with us on that. It is not perfect. We are going to try and get it better and hopefully, it would be something we can implement here down the road.

So, with that in mind, I appreciate the statistics Ms. Cable gave us, 28,000 breaches in the last 10 years. We have a crisis on our hand, do we not? It would seem to me that this is—we have to do something different than what we have done in the past. So, I appreciate your comment. Also when you said data insecurity, that is a new word. I like the way you phrased that. It feels like after 28,000 breaches, we do probably have data insecurity rather than security at this point.

So, with that, Mr. Creighton, I want to begin the questioning with you. There has been a lot of conversation around what this discussion draft might mean for credit bureaus. Can you tell us what if anything would change for your members if this bill was signed into law? And you have two bills here today that address a little bit in your world, so, if you don't mind.

Mr. CREIGHTON. Yes, sure. Your bill, the Data Breach Notification and Security Bill would—we are currently subject to the FTC's Safeguards Rule and our reading of the bill is that we would continue to be subject to the FTC's Safeguards Rule, but we would be subject to a new data breach notification standard at the Federal level, which currently doesn't exist.

Right now, we comply with a series of State laws around the country—

Chairman LUETKEMEYER. That a better deal or a worse deal for you?

Mr. CREIGHTON. Well, I think it would be a greater deal for our consumers, for customers because we are trying to figure out what we should be complying with at any one moment. If there was one strong standard that we could live up to, consumers would benefit from that.

Chairman LUETKEMEYER. OK, very good.

Mr. CREIGHTON. On the PROTECT Act, the most—the biggest change would be the elimination of the use of Social Security numbers in 2 years. We would like to talk to the committee about that. That would not be something that we think we could work with, but we are interested in how we can innovate and how we can get other—find another universal identifier, but it would be a very difficult thing to do.

We haven't solved that problem yet and Congress has been studying it for many years. The other thing is it would set a new data security regulator for the credit bureau industry that would be set by the Federal Financial Institutions Examination Council.

Chairman LUETKEMEYER. Very good. Thank you.

Mr. Kratovil, as you know, financial institutions carry a lot of sensitive information for consumers. Some have charged that those institutions which are subject to the Gramm-Leach-Bliley Act have

no requirements when it comes to safeguards notification. Is that accurate?

Mr. KRATOVIL. In a word, no.

Chairman LUETKEMEYER. I like the brevity of that answer, but I would like a little bit more explanation.

Mr. KRATOVIL. Of course.

Chairman LUETKEMEYER. Thank you.

Mr. KRATOVIL. In 1999, Congress passed GLBA. In 2000, the banking regulators and the FTC began implementing it. What they implemented were a series of interagency guidance and guidelines establishing information security practices and breach notification.

Fundamentally, that guidance was issued as a core element of safety and soundness regulation. Banks are examined to ensure compliance with the guidance and compliance is demanded. And if compliance is not met, examiners have an extensive set of enforcement tools at their disposal which they can ensure any financial institution in violation is compliant.

Chairman LUETKEMEYER. So, I understand that there are all different levels for compliance with this. Are there not?

Mr. KRATOVIL. Yes, sir.

Chairman LUETKEMEYER. I appreciate that. Thank you very much.

Mr. Miller, one of the most discussed elements of the bill deals with requirements of third parties to notify in case of a breach. I think you discussed this a little bit in your opening statement. But can you give us your thoughts on how those requirements should be structured?

Mr. MILLER. Thank you for the question. Well, there are a couple of aspects of the third party requirements that I did point out in my testimony which could be improved.

One of those is with respect to the overlapping requirements between third parties and covered entities. I think this could be tightened up by, I suggested, fixing some of the definitions and focusing both sets of definitions on what types of data is being handled or stored and using terms like that is actually very—it really creates a lot of confusion and, in particular, focusing the covered entity definition on companies that own or license data certainly seems better to us.

With respect to the third party and the notifications themselves, the goal of the bill, we think, should be to provide, of course, meaningful notice to consumers. The entities with whom the consumers have a relationship, if we are really going to effectuate that goal, should be the ones providing that sort of notice. There are always going to be other parties involved in a breach, when we look at today's interconnected ecosystem, and the bill appropriately provides for those parties to work out the details of how those costs are shared.

Chairman LUETKEMEYER. Thank you for that. My time is up. I didn't get a chance to discuss this with you, but just to give you a heads up and hopefully some of the members of the committee will follow up on this. There are some European standards that are being promoted by some of the folks in Europe and I am not a big fan of letting Europe tell us how to do our business over here.

So, I am concerned about that and I will hope that one of our members will follow up with some questions with regards to how you all view those sort of standards and if some of them are good, some of them are not so good, which ones we need to be thinking about.

So, with that, I yield my time to—my time is up and I yield to Mr. Clay, the Ranking Member, for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

Ms. Cable, according to Attorney General Healy, data security and breach notification legislation marked up by this committee last Congress would have drastically undercut your State's data security regulation. Would the concerns raised by AG Healy still apply to the discussion draft under consideration today, and can you explain specifically which Massachusetts safeguards would be undermined if the discussion draft were enacted in this current form?

Ms. CABLE. Thank you for the question. I will say the difference between this bill and prior bills that I think is positive is that it does have a data security minimum standard. In my written testimony, I have included some areas where that standard can be improved in a way that I think decreases compliance cost for businesses and protects consumers.

Putting that aside, the way that this bill changes the status quo in a way that is worse for consumers is, as I mentioned, it doesn't put notice in their hands—mentioned, it does not require notification to consumers until after they have been harmed. It also allows the entity to conduct a preliminary investigation as to the scope of the breach and allows them to take remedial steps to secure the information but puts no outward timeframe for that investigation.

And we believe in our experience, we have certainly seen, this creates opportunities for abuse and further delay before consumers are notified. So, we think that that is a big departure from current law. That does not help consumers at all.

Mr. CLAY. And as the committee considers creating national data security and breach notification standards, can you comment on whether you believe it is critical that we preserve the ability of States to protect their residents from emerging threats to the privacy and security of their data?

Ms. CABLE. It is absolutely critical. Currently, and our office has been actively engaged with our State legislature on improvements and the additional tools that we can use to protect our consumers in light of Equifax, and we are not the only State. I think States have been extremely active after Equifax in taking a look at their security freeze legislation, their data breach notification legislation, they are doing their jobs. They are doing what States do best, which is being agile, being innovative, and coming up with protections that they think fit their consumers and their consumers' needs.

This bill, the preemptive effect of this bill, we think is not in the consumers' interest. And one thing I want to point out about the preemption as it currently is drafted—it preempts any State law, quote, “with respect to securing information from unauthorized access or acquisition.”

It is not limited to securing statutorily defined personal information. There is a big gap between what constitutes information and what constitutes personal information. And in my written testimony, I included some examples of some existing State law that arguably this bill would preempt. That have nothing to do with data breach notification or data security.

I think we are not for weaker Federal standards that preempt stronger State. To the extent there is preemption, we think it needs to be narrowly tailored to the precise matters that the bill is addressing, not spread on other areas.

Mr. CLAY. And, Mr. Chairman, I couldn't agree more with the witness. She is making the point as to why should we weaken current protections under State laws that have already been enacted instead of us erring on the side of trying to craft this bill in a way that is consistent with the strongest protections of what the States have enacted to this point.

I think she makes a great point about that and hopefully going forward, we as a committee can find some common ground in that area. And that is just a comment to you. I haven't finished yet.

But look, it makes sense that we actually err on the side of giving the strongest protection possible to the American consumer and don't weaken them because we are trying to come up with a national law. Don't make it weaker in order to appease one side or the other. Make it stronger. Anyway, my time is up. And I yield back.

Chairman LUETKEMEYER. I appreciate the gentleman's comments and I appreciate Ms. Cable's comments. In fact, the first comment that you made, we are in the process of fixing that as we speak. I think we were aware of that, but we appreciate you bringing that point to us.

Again, we want to make sure that we do this in the right way and, to the gentleman's concerns, this is the reason for the draft, is to come up with better ways of doing things. And we want to hopefully get that done here. Some of the States have some standards that are not able to be adhered to by everybody, so we want to make sure this is something that everybody can live with.

So, we may back off the top standard a little bit to make sure it works, but we are going to try and get this all done. So, again, thank you very much.

With that, we will go to the gentleman who is the Vice Chair of the committee, Mr. Rothfus. He is from Pennsylvania. You are recognized for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

And Mr. Miller, when we look back at the Equifax breach, one of the major questions that stands out is why it took so long to notify the public. Millions of Americans had their personal data compromised and Equifax knew this, but they were not able to take steps to protect themselves some time after the breach occurred because they were unaware.

At the same time, I understand a firm that has been breached goes public before any vulnerabilities can be patched, bad actors can continue to exploit gaps in the firm's cyber defenses. What is the best way to strike a balance between prompt notification and thorough corrective action?

Mr. MILLER. Thank you very much for the question. I think you point out how it is a bit of a paradox. We, of course, want to provide notification as quickly as possible when there is a breach. By the same token, there are a lot of breaches, unfortunately. I think the Chairman mentioned a couple of times already, there is a crisis of sorts. And not all of those breaches are going to actually result in a breach of consumer data.

Organizations have to have the opportunity to conduct an investigation to understand both the scope of the breach and also, in particular, to patch a vulnerability before actually providing notice, particularly public notice to consumers.

So, that is one of the reasons that we advocate against any types of very strict timelines and certainly against an immediate notification, but rather one that is without undue or unreasonable delay, or something like that. Thank you.

Mr. ROTHFUS. Well, the Chairman raised the issue of the European situation with their general data protection regulation and the requirement of a notification within 72 hours. Have you had a chance to take a look at that?

And also Mr. Kratovil, I am just curious what you are thinking on what the Europeans have done. If Mr. Miller, you could comment, then maybe Mr. Kratovil?

Mr. MILLER. Sure, happy to. I have taken a look at the GDPR and that legislation. And I think it points to the importance of really being clear about which notification we are talking about.

There actually is not a 72-hour notification provision in the GDPR with respect to consumer notifications, that there is again an—without undue delay standard there. There is a 72-hour notification obligation where feasible to regulatory authorities. So, again, those are different types of notifications, of course. Thank you.

Mr. ROTHFUS. Mr. Kratovil?

Mr. KRATOVIL. Congressman, I would align myself with Mr. Miller. I completely agree with what he said. No two breaches are the same. If we have learned anything, it is that fact alone, and it does take companies time to get their arms around the breach and to stop the bleeding as it were.

And also to figure out, as Mr. Miller said, did the breach result in something that is actually of harm to consumers? If what was breached was fully encrypted data that is unusable by the person who exfiltrated it from the system and consumers aren't at risk, does that trigger notice? Should that trigger notice? We would argue that it doesn't.

In terms of timing, immediate is arguably an unprecedented concept in terms of speed and certainly among the States. As Mr. Miller said, most rely on some variations on the theme of promptly and without unreasonable delay and we would suggest that that is probably the best way to strike a balance in Federal legislation.

Mr. ROTHFUS. In your testimony, you wrote, "Congress needs to act to require firms of all shapes and sizes that handle sensitive information to protect the data." Why do you believe it is important that firms of all types that handle sensitive data comply?

Mr. KRATOVIL. Thank you for that question. And what I was getting at, I mentioned in my opening statement, you can be a very small business and with modest resources, you can get access to

the technology to allow you to be processing millions and millions of pieces of consumer data.

It is very difficult to say that just based on the size of a company alone should determine how or what data security protection you should have on businesses. That is why the approach in the discussion draft that builds in a flexible and scalable framework that looks at a variety of considerations so that a company can look at itself and make the appropriate decisions based on the type of data that they hold, for example, and how sensitive that data is, as to what cyber protections they need to have in place.

Mr. ROTHFUS. And how would the bill appropriately tailor data security obligations for firms of different sizes and different industries without compromising our collective security?

Mr. KRATOVIL. Yes. It is a great question and you can look even to our law Gramm-Leach-Bliley for some reference and there are parallels with what is in the discussion draft. And as I mentioned, the bill lays out right up front a number of considerations that a firm should take into consideration, such as the size and complexity of the firm, the sensitivity and the type of data it holds, the cost of available products and security.

Again, getting to the idea that you want a small firm that really isn't touching personal information or sensitive financial information should not have the same data security obligations as any of my members of large, nationwide companies.

Mr. ROTHFUS. My time has expired. I yield back.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that, we go to the gentleman from Texas, Mr. Green is recognized. Oh, Mr. Scott. I am sorry.

OK. The distinguished gentleman from Georgia is recognized for 5 minutes.

Mr. SCOTT. Chairman Luetkemeyer, first of all, I want to thank you and Ranking Member Clay for having this very important hearing. Data security is very, very important. It is on the minds of all the American people. And we can do a whole lot better. We better get to work on it very quickly.

And, of course, I represent Georgia, the home of the most unfortunately drastic cyber-attack with a very good company, Equifax, that we are working to get that straight as well.

But, Mr. Chairman, I would like to just address my remarks to one of the pieces of legislation we have before the committee on data security and that is my good friend Congressman McHenry's PROTECT Act, House Resolution 4028.

I just want to trump that and I have had a few moments of being able to talk to Representative McHenry about my concerns on this. And that is that in his bill, I found that one of the problems is that it only requires enhanced cybersecurity supervision for larger consumer reporting agencies.

I think it is very important to realize that Americans have lost faith in all of their credit reporting agencies, so only applying these new standards in his bill to just the largest agencies would mean we would have some agencies that would meet enhanced security standards while others would not.

I wanted to just point that out and see if we cannot build upon that. But more importantly, I want to talk about this organization

that we refer to as the FFIEC. And that organization is the Federal Financial Institution Examination Council.

And that is where we will be passing this hot potato to. It is the interagency council for financial regulators. But I think that this isn't enough. I really think Americans really would want us to go a bit farther.

Everyone should be reminded that most Americans don't have a choice about whether credit reporting agencies like Equifax collect information on you. The American people, their data are the products of these companies.

This world of the credit reporting agencies and how this industry works has been a total mystery to everyone up to this point. And after learning about what is happening, some of the people—American people feel quite a bit helpless and frustrated about it.

Let me just ask you and this panel, with that said, I don't think that the Gramm-Leach-Bliley standards in Mr. McHenry's bill go far enough. And I think we should hold the credit reporting agencies to a higher standard than we have.

We had the worst data breach in American history, 145, 146 million American families lost very valuable data. And so, I was wondering if you all agree with me on this. Ms. Cable, would you respond to that?

Ms. CABLE. Absolutely, thank you for the question. I absolutely agree. In our experience, again, over 10 years, 21,000 data breaches. Equifax is by far the worst. Both in terms of size and scope, the sensitivity of the data and what Equifax is.

It is in the very business of protecting this precise data. And as the full committee learned a few months ago, our office has viewed Equifax through the law. Putting aside the PROTECT Act and looking at the Federal data security proposed legislation, I will note that it does appear to tie the hands of the State against a future breach by an entity such as Equifax. It is a little unclear, but comparing this bill, if it were to go forward, against the status quo, an entity like Equifax would frankly receive a windfall in terms of having one less source of regulators over it and that would be the States.

We don't think that is appropriate at all. We think there is no justification whatsoever, especially in light of Equifax for that to be the case.

Mr. SCOTT. I thank you, Ms. Cable. My time is up. Mr. Chairman, I just make note that I look forward to working with Mr. McHenry on this and see if we can apply it to all of the agencies. I think he will be agreeable to that.

Chairman LUETKEMEYER. Thank you for your thoughtful work here. Thank you, Mr. Scott. His time has expired.

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

Mr. PITTENGER. Thank you, Mr. Chairman for holding this important hearing today. I would like to thank all of you for being here. It has been very revealing for me. Data security is an essential part of any company. It is a critical part of ensuring that consumers' data is protected, that all customers' information is obviously kept safe. I would like to thank, as a result, Mr. McHenry,

Mr. Luetkemeyer, Mrs. Maloney for their efforts and the hard work, all this important legislation.

With the ever-present threat of data breach has many Americans sick and tired of frankly, their Social Security numbers being breached and being identified. And I would like to address first Mr. Miller, and then Mr. Creighton. What can we do about our Social Security numbers being compromised?

Mr. MILLER. Thank you for the question, Congressman Pittenger. Well, I know that the PROTECT Act discusses Social Security numbers and the potential for phasing out Social Security numbers. I think if you talk to most security experts, they will tell you that that is a laudable goal, moving away from static universal identifiers.

The question, of course, as your question implies, is how do we get there? There are all types of innovative technologies and progress being made around different types of authentication using biometrics, et cetera.

I can't sit here today and tell you I have the answer on what the alternative is for protecting or even not using Social Security numbers so much, but I do know that we need to keep looking for other solutions to what Social Security numbers are currently serving in terms of their purpose.

Mr. PITTENGER. Mr. Creighton, would you like to weigh in on this?

Mr. CREIGHTON. Yes, Sir. The Social Security number is really used as an identifier, not as an authenticator. And that is an important difference. You would be surprised at how many people in this country share the same name and even share the same date of birth.

And the Social Security number gives us the ability to match the right information with the right file, for example, a father and a son who share the same name and maybe even the same address.

We believe it is very important that the Social Security number stay out there for identification purposes only. Now, if that was all that was necessary for you to go out and to get a loan, there would be a much greater incidence of new identity fraud or new account fraud in financial institutions because the Social Security number has been compromised so many times that they are out there, right?

The OPM (U.S. Office of Personnel Management) hack, which I was subject to and I am sure others on this committee were, is one example of many other examples where the Social Security number has already been compromised.

The wide-scale usage of Social Security numbers didn't happen overnight. It really was something that is a decades-long process that started with the Executive Branch and eventually moved into the private sector.

But now it is there. And the question that I think we need to answer is, if we are going to replace it what do we replace it with? We still need something that is going to identify people.

Mr. PITTENGER. And?

Mr. CREIGHTON. I don't have the answer for that.

Mr. PITTENGER. OK.

Mr. CREIGHTON. And I wish I did. Believe me because—

Mr. PITTENGER. I thought it was just going to burst out.

Mr. CREIGHTON. Oh no, I wish. But I personally have been breached so many times. It makes you crazy.

Mr. PITTENGER. Sure. I have too—

Mr. CREIGHTON. I understand that, but there is nothing right now that it could be replaced with, unfortunately.

Mr. PITTENGER. We will wait for that magic moment.

Mr. CREIGHTON. Yes, sir. Me too.

Mr. PITTENGER. Mr. Kratovil, kindly tell me the role again, just clarify, of law enforcements and what they play in determining the notification timing after a breach has occurred?

Mr. KRATOVIL. Sure, thanks for that question Congressman. Financial institutions work very, very closely with two primary law enforcement bodies, that would be the Secret Service and the FBI.

They very often maintain very close working relationships with field offices, so that in the event of a cyber incident it can be a mutual effort to help ascertain what has happened, get a handle on the breach. The main purpose of involving law enforcement is to see if they have the capacity in the course of investigating a breach to identify who has done the hacking and maybe even go after them and get them.

And thinking about it in the context of the timing question that we have talked about for notification, it is very important to let that process happen. Our members take engagement with law enforcement very, very seriously. And I know having them involved in an investigation is critical.

Mr. PITTENGER. Mr. Creighton, would you like to weigh in?

Mr. CREIGHTON. Yes and in fact, in some cases, law enforcement actually requests that the breached entity not disclose until they can finish their investigation, and that is something that the law should probably accommodate as well.

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

Chairman LUETKEMEYER. The gentleman's time is about to expire. With that we go to the gentleman from Washington, Mr. Heck is recognized for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman.

Last night I had the pleasure of watching my wife's—whose birthday is today—beloved alma mater, Gonzaga University, put the hurt on BYU, apologies to Congresswoman Love for the WCC championship.

This will be our 19th straight State trip to the dance under Coach Few who is the winningest active coach in the NCAA. And many years ago the big schools started coming after him because of his success. They try to lure him away with a contract a multiple, far away from the little Jesuit University in Spokane, Washington. And he kept saying, "No, no, no, no." And he has said, "No, no, no, no" ever since.

And eventually they stopped asking. And then reporters started asking, why did you say no all those years? And his response was, "Why mess with success?" And that wisdom reminds me of a provision that is included in this draft bill and that is the carve-out for State insurance regulators.

I want to thank the Chair for that. I fought very hard for that last year when we were in the midst of that and extend my grati-

tude to Mrs. Maloney as well. I think it is a recognition that for those of us who have as a goal protecting consumers, acknowledge that State insurance commissioners oftentimes are doing this very well.

I know they are in my State. My goal is protecting consumers and my insurance commissioner is doing that. But that is not to say, of course, that we don't have significant cyber threats in this area.

And so, Sara, I want to direct this to you if I may, Ms. Cable. We are having a hearing on data security. So, if you could suggest to insurance regulators anything that they might do to strengthen their cybersecurity rules, what comes to your mind?

Ms. CABLE. That is a big question. I think I will answer if—

Mr. HECK. It is a great lead-up, though.

Ms. CABLE. It is. It is. I will answer it by saying this is not unique to insurance companies but institutions in general and to comment on a comment made earlier that most breaches are criminal in nature, that has not been our experience. And I think there are other statistics to back this up, but by far most breaches we see are a result of human error because humans are humans.

And sometimes companies have fantastic policies and employees just don't follow them. Oftentimes, however, companies do not have good policies or they have a policy on paper that doesn't actually get implemented.

And even criminal breaches, we see in the case with Equifax, they result because of a failure to do even basic—take even basic security precautions such as patching a software the company knows to be vulnerable.

And so, I think the advice to a regulator would be looking to enhance or enact minimum data security standards, is they are critically important because there is an awful lot of room for improvement.

And I think the standards established in Massachusetts which are similar to the Gramm-Leach-Bliley standards, somewhat similar to those proposed in this bill, although again there are some improvements that we have put forth in our testimony that we think are critical because it is impossible to stop all breaches, but it is definitely possible to stop a lot of them.

Insurance companies handle tremendously sensitive information. Sometimes a company has agents all over the place that they have a hard time getting their arms around in terms of making sure that those agents have secure systems, their computers are secure and what not. So, I do think that data security for insurance companies is critically important. The States have been active in this. We had a resolution against Nationwide Insurance a year so ago.

So, I encourage State insurance commissioners to consider minimum security standards. I think it is critically important.

Mr. HECK. So, in the short period of time I have left, and prefacing this question with the disclosure I am not a lawyer. I note that there is a use of terms like a reasonable risk, economic loss, and unreasonable delay within the notification section of this bill.

As it relates to Equifax, I guess I would be curious, Ms. Cable, if you think 40 days was unreasonable. And does unreasonable delay have any legal meaning?

Ms. CABLE. Thank you for the question. I see my time to answer—we have sued Equifax so I would like to not speak to the specifics on the facts that the timing of the notification is a claim in our case.

But speaking more broadly, Massachusetts has one of those State laws that requires notice, I believe the words are as soon as practicable and without unreasonable delay. It doesn't ascribe an outer limit or initial limit for notice.

And I think that is for good reason. Every breach is different. The circumstances are different. There are times that an entity is not in a position, I have never seen an entity in a position to provide immediate notice. However, I have seen entities in a position to provide notice that delay it for their own purposes. And you can imagine the list of purposes that might be there. Words such as unreasonable, lawyers have a good time with those words.

Ultimately, it would be up to a judge based on the facts and circumstances. So, I think those words are useful, that they provide a flexibility that is not a bad thing for consumers and provides entities the flexibility they need.

Mr. HECK. Thank you.

Chairman LUTKEMEYER. The gentleman's time has expired.

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

Mr. TIPTON. Thank you, Mr. Chairman.

I appreciate the panel being here. I appreciate Congressman Heck's story, which we had a Colorado team that was just winning a championship there as well. But I think you brought up an important point and I think Ms. Cable had pointed to it just a little earlier, brought up Massachusetts, brought up your State regulators in regards to the insurance industry.

And Mr. Kratovil or maybe Mr. Miller, maybe you would like to speak to some of the variances that we do see between different States and maybe speak to why it is important that you spoke to it in terms of some of your testimony, to be able to have some of that harmonization.

Mr. KRATOVIL. Sure. I will start and hand it to my—gentleman, Mr. Miller. I will give you some, at least one example on the security side and one example on the notification side and variances within State laws.

On the one hand, not too many States have data security laws. Of course, Massachusetts has been a leader in that and certainly has arguably the strongest State law on the books right now. As Ms. Cable mentioned, there are many parallels to the Gramm-Leach-Bliley standards for financial institutions in her State's law.

But then you look at other States, for example, that have a data security law that is perhaps just one line, you should have reasonable measures in place to secure data. Those are two ends of the spectrum when you think about data security.

On notice, thinking about the question of timing, I know that is an important topic that the committee is considering. As Ms. Cable noted, her State has what is a variation of a standard that is used by the majority of States, which is something promptly without unreasonable delay.

Some States have chosen to take and set date-specific timelines, say 30 days I think is what the majority of States that have chosen to pick a date have decided to use. So, again, it speaks to the importance of Congress acting here as to smooth out, set the right standard, an appropriately high standard for everyone in the country, because it shouldn't matter where you live as to whether or not your data is kept secure.

Mr. MILLER. Thank you. I agree very much with everything Mr. Kratovil said. Again, just to reiterate the security point, I think it has been pointed out a couple of different times that there are some States such as Massachusetts that do have high security standards in their State laws.

But there are many other States, 30-something, that don't address data security standards at all, so it depends on your perspective, I suppose, when you look at the discussion draft. I would like to take the perspective that the discussion draft is appropriately trying to raise all those 30-something boats up to some type of meaningful, reasonable level for security.

And then on the notification front, again I agree that, in particular, when we are talking about how companies function and have customers in an economy all across the country and the world—their customers are everywhere.

It doesn't make a lot of sense that they are going to have varying requirements with respect to whether it was unreasonable or undue delay, or 30 days or 45 days. So, harmonizing a standard in that regard is really going to improve the purpose of the bill, which is to help consumers.

Mr. TIPTON. Right.

Mr. Kratovil, maybe you could speak to the point in regards to startups and the private sector, private sector businesses. What incentives are in place for them to be able to set cybersecurity regimes within those businesses to make sure that we do have the ability for notification?

Mr. KRATOVIL. I think increasingly privacy and security is being baked in from the moment the coders sit down and start writing the code to make their new technologies feasible. Privacy by design, security by design are starting to become the de facto standard by which entrepreneurs and technologists are building applications. And certainly, from our perspective, FSR's members tend to be on the leading edge of wanting to partner with and collaborate with those technology providers, and when that is the case, certainly our members are going to expect that their technology partners are living up to the absolute highest data security requirements.

Mr. TIPTON. And does that speak to the point where we don't want to have one specific regimen in place to be able to allow that innovation in the private sector for some of the different ideas that can then be shared with others?

Mr. KRATOVIL. Yes. You are absolutely right. Innovation in both cyber and payment security, just as examples, is happening at a tremendous rate. And that is why I keep pointing back to the need, for whatever Congress does in this space to be flexible and scalable. A framework, a process and risk-based framework, that allows that innovation to continue. If you mandate technologies, you just drive everybody to try to comply with what standard you have baked into

the law. That would probably not be in the best interest of innovation.

Mr. TIPTON. Thank you.

And, Mr. Chairman, I appreciate your and Mrs. Maloney and Mr. McHenry's work on a very complex and tough issue that is going to continue to perplex in some areas, but we will be able to make some move forward with this legislation.

Thank you, and I yield back.

Chairman LUETKEMEYER. Thank you for your comments. The gentleman's time has expired.

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

Mr. GREEN. Thank you, Mr. Chairman. I thank the Ranking Member as well. Thank you, the witnesses, for appearing today.

Mr. Chairman, I ask unanimous consent to introduce some 21 letters into the record. These are letters from the American Bankers Association to the Financial Services Roundtable, to the National Association of Realtors, to the U.S. Travel Association, not naming them all. There are many more. With unanimous consent, I ask that they would be introduced.

Chairman LUETKEMEYER. Without objection.

Mr. GREEN. Thank you. And, Mr. Chairman, the Ranking Member breached or broached if you will an area that I would like to go into. And in so doing, I would like to lay this predicate. There is an industry perspective on this.

And it appears that the retailers, and I am reading now from the briefing book, have cautioned against replacing State standards with the weaker Federal standard. There is also an indication from the intelligence shared that consumer advocates of the opinion that a national data breach notification standard should not come at the expense of weakening the strongest standards already afforded in other States.

So, my question is to you, in your opinion is the discussion draft a floor or a ceiling? And each of you can respond if you like. Well, why don't we start here with a show of hands first. If you think it is a floor, would you kindly raise your hand.

And if you don't understand what a floor is, you can raise your hand and then I will say more. Or if you think it is a ceiling, raise your hand. OK. It seems we have unanimous consent that it is a ceiling.

If you would, let us start with Ms. Cable, why, in your opinion, is a ceiling appropriate or inappropriate?

Ms. CABLE. Well, our position, perhaps not surprisingly, is a ceiling is inappropriate particularly in this realm. This is fundamentally drafted as a consumer protection measure. And for a variety of reasons set forth today and I suspect in the letters that were just submitted for the record, there are a variety of ways this bill offers weaker protections than currently are available to consumers under State law.

And in light of Equifax, there appears no reason from our perspective to do so by then preempting States from enacting stronger protections or enforcing the existing strong protections that they have.

It is really just locking consumers into a weaker set of protections for the foreseeable future at a time when breaches, risks continue to multiply. So, we are not in favor of a ceiling of protections.

Mr. GREEN. And your name is Cable not Gable.

Ms. CABLE. Cable, yes.

Mr. GREEN. Thank you.

Let us move on to Mr. Miller. Mr. Miller, I believe you would contend that it is appropriate to have a ceiling, is that correct?

Mr. MILLER. I guess I would—yes?

Mr. GREEN. Mr. Miller, I am going to have to ask that you not equivocate if you would.

Mr. MILLER. OK.

Mr. GREEN. Are you a ceiling guy or are you a floor guy?

Mr. MILLER. Well, I think the bill tries to be both a floor and a ceiling—

Mr. GREEN. Mr. Miller, Mr. Miller. I know. But the bill has to be a ceiling or a floor. It really does. So, this may be a time for you to pick sides.

Mr. MILLER. I think we want to have a common notification standard, and I think—

Mr. GREEN. Let me ask another question, Mr. Miller. Let me go on to another question. Do you think that there should be some language somewhere indicating that if there is a breach, you cannot sell your stock if you are one of the executives? You can't sell your stock before you announce the breach. Should there be such language?

Mr. MILLER. I am not sure if that language should be in this bill or not, but it seems like a secure—

Mr. GREEN. But, no, no, but Mr. Miller—

Mr. MILLER. —that sounds security—

Mr. GREEN. If you will note, I said some place.

Mr. MILLER. OK.

Mr. GREEN. OK, some appropriate place because this is what happened.

Mr. MILLER. Right.

Mr. GREEN. And if you think that there should be some language, we know that security laws can deal with it, but should there be some language that specifically says if there is a breach you can't sell your stock before you announce the breach?

Mr. MILLER. That seems like reasonable guidance.

Mr. GREEN. Raise your hand if you think that there should be such language. Yes, raise your hand please. That is all right. OK. Everybody. So, I see that we have one person who did not.

Sir, would you explain why you don't think so?

Mr. CREIGHTON. Selling stock based on material nonpublic information is illegal. And this is under investigation. And if they were aware of a breach and they sold their shares based on that that is something that the SEC and other Federal—

Mr. GREEN. I understand there are agencies and entities that will look into it, but given that it happened and we can put people on notice, is it so redundant that it would be harmful? Is it so superfluous to the extent that it makes no sense? It just seems that it is OK to tell people if you do this, there is a penalty.

Mr. CREIGHTON. It is already illegal. And I wouldn't have any objection to it, but it is already illegal.

Mr. GREEN. OK. Thank you, Mr. Chairman.

Chairman LUTKEMEYER. The gentleman's time has expired.

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

Mr. WILLIAMS. Thank you, Mr. Chairman.

And thank you to the witnesses today that are here. As this committee continues to work to protect American businesses and consumers that are under a constant threat from cyber thieves, as we have seen in the past year, cybersecurity breaches and a loss of personal identifiable information have unfortunately affected hundreds of millions of Americans.

Mr. Kratovil, in your testimony you state that this legislation strikes the appropriate balance by setting a high bar for data protection while providing numerous considerations to ensure a small business that processes or maintains little or no personal information is not burdened with the same expectations as a large entity.

As a small business owner myself for over 47 years and a steadfast defender of Main Street, I appreciate what you have to say about that. My question is, what importance does scalability play in ensuring a level playing field for entities of all sizes and how does this affect consumer protection?

Mr. KRATOVIL. Thank you for that question, Congressman. It is one of the critical aspects that we believe should be included in any Federal legislation in this space. Scalability, flexibility—taking into consideration the size and complexity of a business—all has to be weighed in evaluating which cybersecurity resources a company should be deploying.

If you were an FSR member, I think there are going to be—there certainly are regulatory expectations that you are investing heavily in cyber defenses. I know just a handful of our members have invested over \$1.5 billion a year in cybersecurity defenses.

Juxtapose that against small businesses, perhaps such as your own. When you look at your business, perhaps you are not even—your employees aren't even coming into contact with sensitive financial information that would be covered under this legislation.

It probably goes without saying then, you should not be employing the same cybersecurity resources as a national bank, for example.

Mr. WILLIAMS. OK. Another question for you. In your testimony you state that legislation should recognize both the danger of alerting hackers to vulnerabilities before they have been remediated and risking potential further harm to customers, and then the risk of confusing or alarming consumers unnecessarily if companies are forced to notify prematurely. So, why is that important?

Mr. KRATOVIL. The idea there, is that oftentimes, when a company discovers that they have been hacked, it is often the case that the hackers are still in their systems. That is why in the legislation it makes clear that hopefully law enforcement is going to be able to be involved in a situation like that and law enforcement may have an opportunity to trace where the hack is coming from. Maybe even to identify who is doing the hacking, in which case you definitely want to be able to allow that process to happen.

Mr. WILLIAMS. OK.

Mr. Creighton, the Senate has proposed limiting the amount in type of data that can be reported about consumers to credit bureaus. My question is, what effect would these types of restrictions have on the accuracy of consumer lending decisions? And how would they affect credit availability, particularly for vulnerable populations?

Mr. CREIGHTON. Thank you for that question. When we collect data, we are trying to collect data that is going to matter for a future lending or other decision. Those kinds of data are what kind of accounts do you have? What is your credit limit? How much credit are you using? Do you pay on time? Those kinds of questions.

We are trying to continue to gather more information from other kinds of data furnishers—home renting companies, apartment companies, that kind of thing, cell phone companies, others so that we can expand the number of people who have thin files.

Because if you have a thin file right now, and you go to get a loan, they will look and they say, “Well, we don’t know enough information about you to know whether you are a good risk or not.”

So, we want to get more of that information because if we have more of that kind of information, we are going to do a better job of giving lenders what they need so that they can bring people into the regulated financial system, which is what we are all after.

Mr. WILLIAMS. Good. Another question to you. In your testimony you stated that credit reporting agencies face only enforcement and not supervisory and examinations by the FTC. So, why do you believe that empowering the FFIEC to choose the correct overseer is the proper fix for this regulatory gap?

Mr. CREIGHTON. Yes. Thank you for that question. In the time since I submitted my testimony, what I have learned from my companies is that actually the Consumer Financial Protection Bureau has asserted its authority under UDAP (unfair or deceptive acts or practices) and other provisions to begin examination of credit reporting agencies on cybersecurity.

While the GLBA specifically says that cybersecurity is carved out under UDAP authority, the CFPB has asserted its authority and is now examining at least two of our companies.

Mr. WILLIAMS. OK. Thank you for being here. And I yield back my remainder of my time back.

Chairman LUETKEMEYER. The gentleman yields back his time.

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

Mr. LOUDERMILK. Well, thank you, Mr. Chairman. I appreciate the panel being here today.

Mr. Kratovil, as I understand it, the Gramm-Leach-Bliley Act may not explicitly require financial institutions to comply with mandatory Federal data security and breach notification requirements, but these requirements are essentially mandatory in practice. Can you explain how that happens?

Mr. KRATOVIL. Yes. Thank you for that question. And yes, sir, I agree with you. They are mandatory. There is nothing about Gramm-Leach-Bliley’s security requirements or notice requirements that are treated as optional.

As I mentioned earlier to the Chairman, fundamentally, these are safety and soundness standards. They are treated as such for examination purposes. Examiners view compliance with both the security requirements and notice obligations as affirmative duties under safety and soundness regulations, and the examiners themselves have a variety of enforcement tools at their disposal should they find a firm is not living up to either of those obligations.

Mr. LOUDERMILK. OK, I appreciate that. I had my staff ask the Congressional Research Service and they advised the same thing, and so, I just want make sure that we had a good understanding of that and I appreciate that.

Mr. Miller, I want to talk about the third party liability issue. I understand both sides of this debate. And on the one hand, understand the—and I appreciate the argument that the company that is breached should be responsible for the notification, but on the other hand, are we subjecting the consumers to even more or greater risk by transferring more data into an entity that was just breached. I am trying to find a good medium there. Can you comment on that?

Mr. MILLER. I just want to make sure I understand your question, you are talking about transferees of more data to third party because of this breach—

Mr. LOUDERMILK. Well, in a third party situation where there was a breach but the third party may not have the contact information. And if we require them to actually make the notification, are we not risking the consumer by even sending more data to that third party?

Mr. MILLER. Absolutely, particularly if the third party is the one who was breached. Probably there are questions regarding security, so sending a bunch of additional information to them seems questionable.

Mr. LOUDERMILK. Yes. And I feel like there is some liability there, but then we have that issue, and I don't know if anybody else would like to comment on that if you have feelings, it is just one of those, that they are issues we are struggling with at this point, of how do we resolve that if they were, the third party was actually the factor that caused the breach.

Mr. MILLER. If I could just comment a little bit further on the third party, it is true that third parties, again, if we look at business arrangements and particularly of large companies across a variety of industries, they are using third parties for a variety of different purposes. Some of those third parties are small companies, some of those third parties are large companies and providing all different types of services.

There was one very notorious breach a few years ago where a major company was breached through a third-party HVAC vendor for instance.

Mr. LOUDERMILK. Right.

Mr. MILLER. So, the most sensible way it seems to deal with the apportionment of liability in these types of scenarios is through a contractual arrangement between the parties who are free to contract with different parties if they would like to choose different entities with which to work and requiring strong security practices is certainly something I would advise any party to do.

Mr. LOUDERMILK. OK. I appreciate that. This is one of the issues that I have been struggling with because I understand that there is some liability there but also do you provide more information to the entity that was just breached.

And dealing with the information, I will throw this out to anyone in the panel in the last few seconds we have, are we collecting and maintaining too much data, because we know the more data you have the more data we require through the Government to be maintained, the more risky it is when you don't have to protect what you don't have.

Anyone want to comment on are we collecting and maintaining too much data?

Ms. CABLE. I think your point is well stated. If you don't have it you have automatically reduced the risks to your company.

I can't speak to, I know that it is extremely valuable to businesses and it provides benefits for consumers for those businesses to have that data. However, we do see a lot of companies collecting data that is very sensitive for consumers without having a present need for it or holding on to data for years and years and years when they are not using it. So, I do think that is part of the concern, good practice, data management practices would reduce the amount of data that you are not using that you don't have.

Mr. LOUDERMILK. Well, I appreciate that and I think that would expand also to our Government as well.

Mr. CREIGHTON. Very briefly I was just going to make that same point. This is a problem across the economy in both public and private sectors.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that we go to the gentlelady from Utah, Mrs. Love is recognized for 5 minutes.

Mrs. LOVE. Thank you.

Do the standards for credit bureaus differ from the standards for other sectors of the economy? If so how, why, and I want to get into the European cybersecurity initiatives just to follow up from the Chairman's questions.

Mr. CREIGHTON. Sure, the National Credit Reporting Agencies are subject to the FTC's Safeguards Rule, which is the rule that applies to, under the Gramm-Leach-Bliley Act, to non-bank financial entities. So, there is no data security standard for most companies in the country, but financial institutions have standards. So, if you are a bank you are covered by your prudential regulator but if you don't have a prudential regulator like the OCC or the Federal Reserve, then you are subject to the FTC's Safeguards Rule. And the credit bureaus are one kind of company that is subject to that.

Mrs. LOVE. OK. So, I guess this is an opinion for everyone. I am interested in the European standards, how do you view these standards? Do you think that these standards are going to be influential? I just wanted to follow up because I think that, I agree with the Chairman, I would hate to have somebody else dictate what we do. So, I just wanted to know what your thoughts were on that.

And anyone can answer. I am just—

Mr. CREIGHTON. I will kick it off because I will be very brief. Generally speaking, our reading is that for credit bureaus specifi-

cally there would not be much impact from it because we are collecting as credit bureaus very narrow parts of the larger information environment. Again, as I said, we are collecting the “do you have credit, how much credit, with whom, do you pay on time?” And those sorts of—that sort of information is part of an ongoing business relationship that you have with your lender.

So, if you have a credit card account, that credit card company is reporting that information up and that would continue even under GDPR. The larger data broker issue would come into—is more implicated by that and that is not a part of the environment that I generally work in.

Mrs. LOVE. OK.

Mr. MILLER. Thanks for the question. With respect to the GDPR there are a few different requirements particular to breach.

As I mentioned previously, there is a “without undue delay” standard for consumers and with respect to notifications to regulatory authorities there is “where feasible, but not later than 72 hours” language.

I would additionally say this, to speak to the Chairman’s question that he teed up at the outset, it is premature to be looking to the GDPR as a best practice for anything, in my opinion, to the extent that it hasn’t been implemented yet. It is going to be implemented this May. There are a lot of questions regarding how certain provisions are going to be implemented, particularly around data breach. So, I would say—I wouldn’t worry too much yet about that particular issue.

There are also a variety of cybersecurity standards in Europe that are being proposed that I would also be happy to get into, but—

Mrs. LOVE. Is it important to keep an eye on that and to look on how that affects?

Mr. MILLER. It is definitely important because, again, all of our companies are global companies doing business globally, so they are going to have to comply with that if they are doing business in Europe, or doing business with European citizens. So, it is important.

I am just commenting on, not looking to something that hasn’t yet been implemented, to see if it can be implemented as designed, as a model. I think it is premature to do that.

Mrs. LOVE. Do you have any concerns with the present model? I know you are concerned about because you don’t know how it is going to be, what the reaction is going to be or what the results are going to be, but do you have concerns with the way that it is set up and what the standards are currently?

Mr. MILLER. Well, again, as the number of—I think all the witnesses have said at one point or another today having a very tight timeline for any notification such as 72 hours is very problematic just because, again, as we can point to lots and lots of high-profile breaches, you can look at some Government breaches like OPM, it takes months sometimes to even realize there has been a breach and then to figure out what exactly is going on.

So, a 72-hour provision in many instances is going to be impossible to comply with.

Mrs. LOVE. Do they have that in their standard, they have a 72-hour—

Mr. MILLER. Yes, the 72 hour for notification to regulators but not for notification to citizens.

Mrs. LOVE. OK. Do you have anything that—you mentioned, you look like you had something that you wanted to add.

Mr. KRATOVIL. I would just agree on what Mr. Miller, the point he made about it might be a little too early to make any judgment calls on GDPR. I know many of FSR's members are global in nature, and so, it is already, there is already a tremendous amount of discussion as to how do we come into compliance with this and make that system work.

Mrs. LOVE. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman LUETKEMEYER. The gentelady's time has expired.

With that we go to the gentelady from New York, Ms. Tenney is recognized for 5 minutes.

Ms. TENNEY. Thank you, Mr. Chairman.

And thank you, panel, for this discussion. As we know, obviously, cybersecurity, cyber attacks are becoming the new way to rob a bank, to rob a store, to rob citizens from their living room.

Last year, the New York City Attorney General reported 16 percent, or that cybersecurity invasions are up 60 percent, and more and more of New York's personal records, in fact, have been tripled since last year. Obviously the Equifax breach was huge for us with eight million people in New York State being exposed in the Equifax breach out of about 19 million.

Actually, this past January, our own New York State Education Department was also breached. These things are certainly of concern. I want to just give a little shout-out to a local college in my community. Utica College has teamed up with the cybersecurity department in our county to try to prevent against these attacks and identify potential risks and weaknesses in our data system.

But my question involves, first, I would just like to find out to what extent will a national standard provide for better security than something on the local or State level?

Obviously, I am just curious if you could comment, maybe Mr. Kratovil, you could mention it first?

Mr. KRATOVIL. Sure. Thank you very much for the question.

If it is done correctly and by that I mean if it is an appropriately strong standard, as we have talked about a lot, it takes into consideration a variety of factors to not overly burden small businesses, we believe that is the absolute best way for Congress to act to ensure that no matter where you live in the country, that your data is protected with a strong standard. That is really the core for the financial industry.

Ms. TENNEY. Great. And I think it is great that we are tackling this issue but I am a small business owner, and so, for us, obviously our customers and their security is of paramount interest to us like smaller banking institutions and other types of retailers.

So, how can we make this in a way that is cost effective so that the smaller players which often can't afford the compliance costs of a national standard, how do we come up with something that is affordable to them because what often happens is you come up with

a national standard and then these people will get left on the way-side and then you end up with the collapse of the small business community because they just can't—this is a perpetual problem in State government. I know when I was in State government, we just put these big one-size-fits-all regulations and then we ended up with the loss of a small business community, which is really important to our area.

Mr. KRATOVIL. Yes, that is a very important point and I am glad you raised it. And the discussion draft actually gets right to the heart of the cost question, because securing data is not a cheap proposition. And 3.A.2.c reads the cost of available tools to improve security and reduce vulnerabilities.

Ms. TENNEY. Is there enough flexibility in this standard that would allow groups, different retail groups or different sectors, to get together in a way that they could provide for their own security and to manage the costs? Is that something that has been contemplated and anyone on the panel can comment on that quickly if you have a question, without violating any kind of Federal standard.

I know there is a lot of—obviously we are dealing with Social Security numbers and sensitive information which is—which is in there. Anyone have a comment on that? There is no way to make that so that they are able to do, to be able to collaborate or come up with a retail institution?

Mr. CREIGHTON. I am probably not the best person to talk but the establishment of sector-specific ISACs (information sharing analysis centers)—

Ms. TENNEY. Right, OK.

Mr. CREIGHTON. —is really the best way for companies to be able to share information, build relationships with Government and to prepare for breaches and then respond to them. And there—we have them in financial services, energy, lots of different entities.

Mr. MILLER. Yes. There are several dozens of ISACs in the country.

Ms. TENNEY. Right.

Mr. MILLER. Financial services ISAC includes thousands and thousands of financial institutions in the country. Retail ISAC was stood up in the last few years. Again, to Mr. Creighton's point, to be able to share that threat information and help each other defend against cyber attacks.

Ms. TENNEY. Right. And I think that should be helpful. Obviously it is sensitive information.

One of the big concerns I have is just a little bit outside of this space, is that we have—the State governments typically don't have the ability and the resources to provide really adequate security and data. Do you think that that is something that could be done—so we have a national standard, what about the State government's requiring some of these data be turned over in the regulator process, for example, the banking institutions, insurance institutions, and other retailers?

Mr. KRATOVIL. Well, we have many of those same concerns at the Federal level because the bank regulators do expect tremendous amounts of very sensitive and proprietary information, for example,

about financial institutions' cybersecurity programs to be turned over as part of the examination process.

Ms. TENNEY. I am running out of time, but one quick thing, for example, Congress gets hit almost every day and the Government institutions are probably the most vulnerable. Would you agree or disagree?

Mr. KRATOVIL. Yes, ma'am, I would agree with that.

Ms. TENNEY. Thank you so much. I appreciate your testimony. Thanks.

Chairman LUETKEMEYER. The gentlelady's time has expired.

With that we will go to the gentleman from Michigan, Mr. Trott is recognized for 5 minutes.

Mr. TROTT. Thank you, Chairman.

I want to thank the panel for joining us this afternoon. And one of my concerns when we work on data security and standards is a desire, on the part of some, to set up "gotcha" moments. And if you look at the Equifax breach, terrible set of facts but it provides good 30-second soundbites for people here in D.C. to attack Equifax and they deserve some of it, that is for certain.

But one of my concerns and I would be interested in, Mr. Miller, your thoughts on whether either bill that we are looking at, are the standards reasonable? And I know section 3 of the Chairman's bill says, "reasonably designed to protect individuals."

If you start with the premise that no business or database including the Government is beyond being hacked. When I was in business we used to hire brilliant high school students to figure out a way to hack into our firewall and our databases. And they always seem to figure out a way to do it, and we spend a lot of money on trying to protect our data.

But do you feel like there is enough flexibility such that some of these businesses aren't being set up to fail?

Mr. MILLER. Thank you for the question. I think for the most part, there is a significant amount of flexibility in the security standards in the bill and that is appropriate. As others on the panel have said, it is really important that we aren't too prescriptive in our standards and require the same level of specific security standard for a large multinational corporation or the Department of Defense, as we do for a small or medium-sized business or a startup. There are a whole bunch of reasons for that.

In particular, one of the good things about the list of safeguards in the bill, is that they are consistent with a lot of risk management-based principles, and while we certainly advocate for risk-based approaches, I think it is important that we also, when we talk about data security, we often talk about the protect function and that piece of the puzzle, and that is really important.

But there is the reality that breaches are going to happen so you need to be focusing also on how you respond and how you recover from that breach, and that is the bill.

The one thing in the safeguard section that does seem to not really account for that sort of flexibility to us is the requirement to have, essentially, to designate a security official who is in charge of the safeguards.

Again, if you have a two-person startup it is questionable whether you need to have the same type of mechanism, a designated se-

curity official at a two-person company or at a major bank, for instance. And that is the one thing I would say about that.

Mr. TROTT. Yes the two-person startup, the designated person might also be cleaning the coffee pot out at night, too. So, that is a problem.

One question, this area is constantly evolving, so what kind of flexibility should we build into any solution to deal with the changes that are inevitable with respect to the technology and how consumers are using the Internet and other places where they are putting their confidential information?

Any thoughts would be helpful, because there is no question that today's safeguard is going to be updated tomorrow when they figure out some other new and better way to hack into it.

Mr. MILLER. Well, I completely agree with that. We want to have technology-neutral requirements. The point was made earlier about innovation and the fact that there are new security measures and tools being developed all the time. And it is obviously something that we need to do, because the attackers are also innovating and coming up with new techniques.

There are plenty of examples that we probably don't have time for now. But, there are security technologies that were state-of-the-art 10 years ago that simply aren't state-of-the-art today. If you bake those into a statute and say you must use technology X eventually that is going to be an obsolete statute.

Mr. TROTT. No question.

Mr. Creighton, you I think mentioned the CFPB a few minutes ago, can you just briefly comment on how the decisions by the CFPB and the FTC and other banking regulators have conflicted in this area? And maybe this was covered earlier by someone—I got delayed getting here—and, do you think that UDAP authority that the CFPB utilized is even appropriate?

Mr. CREIGHTON. Well, in GLBA, in Dodd-Frank the data security was specifically carved out of the CFPB's authority. And we would suggest that Congress would probably want to revisit that as the McHenry bill does, as the PROTECT Act does. But the CFPB does and always has maintained UDAP authority and they are in the process now of asserting that authority and getting in there, and, if they are in there, they are in there. We are not in the business of criticizing our regulators.

Mr. TROTT. Yes. OK. I will do that for you, so no worries.

But I think I am about out of time so I yield back. Thank you again for your time, gentlemen.

Chairman LUETKEMEYER. The gentleman yields back.

We are without any further folks in the queue. So, with that we will wrap up the hearing.

Just some closing comments. We were discussing today the ability to protect consumers' data. We also need to be able to allow them not only to be protected, we also need it to be accessible by them. And when we do that it makes it very difficult to have both at the same time. This is where you can't lock it up and you have to be accessible to it but that makes it vulnerable, so how can we protect the data? That is the trick.

One of the questions that we were working here throughout the discussion was with an immediate notification. I knew coming in

this was going to be a discussion point and I left it there intentionally to get everybody started, and I appreciate the discussion we had. But I am a little disappointed because in the bill it says, the draft bill, that you don't notify until you recognize that you had a breach, until you make sure that an individual person's information has been breached, who that person is, and where that person is something that could cause—that information could cause a loss.

Therefore you are not notifying immediately when a breach occurs, you are notifying exactly whenever you determine that there is a reasonable expectation that the data that was breached was for an individual that could suffer a loss. And so I am a little disappointed with the comments that were made.

Obviously, everybody wants to have as much time as they can to resolve the situation, but I can tell you that this is a touch-point for a lot of my constituents, your customers. They want to be able to protect their data as quickly as possible. I can tell you that when we put in there reasonable or expeditious or something that somebody could drive a truck through, they are not going to be happy, because they want to be able to have confidence that their information is going to be protected and they will have access to it and be able to protect it themselves if necessary and as quickly as possible.

So, we want to work with you on that language to try and make sure this works, and we thank you for your thoughtful suggestions along all the lines.

Ms. Cable has made some great suggestions. We realize you have a strong standard and we appreciate that.

We have to find a balance somewhere in all of this where we can be, as Mr. Kratovil continuously said, flexible, scalable, and have some balance to what we do so it can be something that everybody all along, the scale here can actually use this information and do something that we think is productive.

I have been tasked with putting this bill together by leadership because of the thousands of breaches that have occurred.

Ms. Cable's testimony indicated 28,000 over the last 10 years, it was 1,700 last year; something has to be done. We are, I think, close to a crisis situation here, and quite frankly we are one major breach away from this new legislation being fast-tracked, quite frankly. So, I think that everybody here today appreciated the large audience that we had.

I think that we are all going to continue to work together to get this bill to a point where it is a good bill or something that we can address as many of the concerns that we can get to. Or it is going to be a very difficult bill to get everybody to yes. We want to get everybody to neutral if possible and a yes. We are going to continue to work with everybody and we appreciate your suggestions, but again, I want to emphasize we are one breach away from this being a bill that is going to be dropped and we are going to run it, because our constituents are going to demand it and we are going to be in the cross-hairs.

So, with that thank you so much for your time today. Thank you for your testimony and I appreciate your participation. I have some final comments. Here we go.

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

[Whereupon, at 3:53 p.m., the committee was adjourned.]

A P P E N D I X

March 7, 2018



MAURA HEALEY
ATTORNEY GENERAL

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

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

**Prepared Statement of Sara Cable
Assistant Attorney General and Director of Data Privacy & Security
Consumer Protection Division
Office of the Massachusetts Attorney General**

**Before the House of Representatives
Subcommittee on Financial Institutions and Consumer Credit**

**Hearing Entitled "Legislative Proposals to Reform the
Current Data Security and Breach Notification Regulatory Regime"**

March 7, 2018

Introduction

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee, thank you for inviting me to testify today regarding the discussion draft bill, entitled the Data Acquisition and Technology Accountability and Security Act, dated February 16, 2018 (the "Bill"). I am an Assistant Attorney General for the Massachusetts Attorney General's Office, and the Director of Data Privacy and Security for its Consumer Protection Division. On behalf of the Office, I appreciate the opportunity to share our experience over the past decade enforcing the Massachusetts Data Breach Notice Law and Data Security Regulations (Mass. Gen. Laws c. 93H; 201 CMR 17.00 *et seq.*).

We applaud the Subcommittee's recognition of the importance of strong data security protections and breach disclosure obligations. It seems every day consumers learn of a new data breach at yet another well-known company: TJX, Sony, Adobe, Target, Home Depot, Yahoo!, Anthem, Uber, and Equifax, just to name a few. These occurrences seem so common, they feel inevitable, a sentiment encapsulated by the oft-stated warning of cybersecurity professionals: "it is not a question of whether a breach will happen, but when."

The recent news of the Equifax breach—which put 145.5 million Americans at risk of identity theft and financial fraud—has once again brought this issue to the forefront of the public consciousness. Equifax may be the latest massive breach, but if history is any guide, it will not be the last. That a company in the very business of safeguarding and managing vast troves of the most sensitive consumer data failed to protect it despite knowing that its systems were vulnerable

to hackers makes clear that more must be done to protect consumers and preserve their confidence in the market.

Now is not the time to dilute or preempt the tools regularly and successfully used by many states, including Massachusetts, to combat this crisis. Especially in light of breaches like Equifax, this is the time to build on and improve existing protections under federal and state law. This Subcommittee's first priority should be protecting consumers from the dangers posed by data breaches, not minimizing compliance costs for businesses that allow breaches to occur. Congress should not expose American consumers to increased risks as a result of a new, less stringent national standard.

For the past decade, the Massachusetts Attorney General's Office, along with its sister States, have been on the front lines on this cybersecurity problem. We help consumers in the aftermath of a breach as they struggle to protect themselves from identity theft, fraud, or other harms. We engage with business on a regular basis, providing guidance on compliance with the Massachusetts Data Breach Notice Law and Data Security Regulations, and educating them on emerging cybersecurity threats and strategies to avoid them. And through the Massachusetts Consumer Protection Act and Data Breach Notification Law, we hold companies accountable when they fail to comply with our law and keep consumers' data safe from foreseeable threats.

As the "cop on the beat" working on the front lines of the data security problem, we believe that this Bill, taken as a whole, will leave consumers in a worse position than the status quo. As I will describe below, this Bill allows entities to push the cost of the data security crisis onto consumers without providing any meaningful remedy, strips the state Attorneys General of the authority they are presently and actively using to protect their consumers from breaches, and hamstring efforts of the States to enact laws in response to future risks in an era of increasing and rapidly evolving technology.

Discussion

I. The Bill Makes It Harder for State Attorneys General—the "Cops on the Beat"—to Do Their Jobs.

a. Direct Notice to State Regulators Is Essential.

The Massachusetts Data Breach Notice Law and Data Security Regulations are recognized as among the strongest in the nation. Together, they protect consumers by requiring entities that own or license "personal information"¹ of Massachusetts residents to develop, implement, and maintain minimum security safeguards to protect such information from foreseeable threats and from unauthorized access or use.² If such information is breached,

¹ In Massachusetts, "personal information" is defined as a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. See Mass. Gen. Laws. c. 93H, §1 (**Exhibit 1**).

² See Mass. Gen. Laws c. 93H (the Massachusetts Data Breach Notice Law); 201 C.M.R. 17.00 *et seq.* ("Standards for the Protection of Personal Information of Residents of the Commonwealth") (the Massachusetts Data Security Regulations), and Mass. Gen. Laws. c. 93I (the Massachusetts Data Disposal Law) (**Exhibits 1-3**).

Massachusetts law obligates entities to notify, “as soon as practicable and without unreasonable delay” each affected resident, as well as other state agencies, including the Attorney General.³

Over the last decade, over 21,000 data breaches have been reported to our Office under the Massachusetts Data Breach Notice law, and over ten million data breach notifications have been sent to Massachusetts consumers. In 2017 alone, over 3,800 breaches were reported to our Office. Direct notice of breaches to our Office is a critical component of our law. It allows us to ensure that consumers are promptly and properly notified so that they can take steps to protect themselves from resulting identity theft or fraud. Direct notice also allows us to engage in education and outreach to the business community to increase awareness of the importance of data security. Finally, it gives our Office an informed and comprehensive view into the nature, extent, and frequency of breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

As currently drafted, the Bill unwisely does away with direct notice of breaches to state Attorneys General for those breaches that impact their residents. This is in direct contrast to the current requirements under Massachusetts Law, and the laws of twenty-four other states.⁴ Such a change to the status quo would directly and significantly impact our ability to protect our residents. In the absence of direct notice, any given state Attorney General instead would have to rely on individual consumers, media, or whistleblowers to bring breaches to their attention, an impractical approach that forces a state Attorney General Office to navigate delays and unnecessary burdens to obtain information about the overall scope of a breach and its impact on state residents. A better solution that also promotes the interests of consumers is to require entities to directly notify state Attorneys General of breaches impacting their state’s residents, as many state laws already require.

In addition, the Bill’s proposed threshold for notice to federal regulators (breaches that impact 5,000 or more consumers of any state) is likely not to capture the vast majority breaches that, while not nationally significant in size, may have a significant impact on the residents of a particular state. For example, in Massachusetts, *less than 1%* of the over 3,800 data breaches reported to our Office in 2017 impacted 5,000 or more Massachusetts consumers. Indeed, over 93% of the over 3,800 breaches impacted fewer than 100 residents each. Assuming similar statistics in other states, the Bill risks creating an enforcement “blind spot” for both state and federal regulators, who would not receive notice of the vast majority of data breaches that occur. While such thresholds may work for large breaches that affect consumers nationwide, it does not work for breaches that affect only one state or region.

³ See Mass. Gen. Laws c. 93H, § 3(b) (**Exhibit 1**).

⁴ See Cal Civ. Code § 1798.82; Conn. Gen. Stat. § 36a-701b; Fla. Stat. § 501.171; H.R.S. § 487N-1 *et seq.*; Idaho Code § 28-51-104 *et seq.*; Iowa Code § 715C.1-2; La. Rev. Stat. § 51:3071 *et seq.*; 10 Me. Rev. Stat. § 1346 *et seq.*; Md. Code Com. Law § 14-3501 *et seq.*; Mass. Gen. Laws c. 93H § 3(b); Mo. Rev. Stat. § 407.1500; Mont. Code § 30-14-1701 *et seq.*; Neb. Rev. Stat. § 87-801 *et seq.*; N.H. Rev. Stat. § 359-C:19 *et seq.*; N.J. Stat. § 56:8-163; [NM] H.B. 15 (signed into law April 6, 2017); N.Y. Gen. Bus. Law § 899-aa; N.C. Gen. Stat. §§ 75-61, 75-65; N.D. Cent. Code § 51-30-01 *et seq.*; Or. Rev. Stat. §§ 646A.604; R.I. Gen. Laws § 11-49.2-1 *et seq.*; S.C. Code § 39-1-90; 9 V.S.A. §§ 2430, 2435; Va. Code § 18.2-186.6; and Wash. Rev. Code § 19.255.010 *et seq.*

b. The Bill's Enforcement Mechanisms (Section 5) Hinder the States' Ability to Protect Their Consumers.

Also critical to our consumer protection efforts is our authority to investigate the circumstances of data breaches, and where appropriate, enforce the Massachusetts Data Breach Notice Law and Data Security Regulations. This authority derives primarily from the Massachusetts Consumer Protection Law (Mass. Gen. Laws c. 93A). We do so in situations where the circumstances of a breach reflect gross failures by an entity to implement or maintain basic security practices, where the entity unreasonably delayed providing notice of the breach, or other egregious conduct that raises real risks of resulting consumer harm. This enforcement authority allows us to obtain restitution for those consumers who suffered ascertainable losses, and deter wrongdoing by companies in the future through civil penalties and injunctive relief.

For example, on September 19, 2017, this Office filed suit against Equifax under our Consumer Protection and Data Breach Notice laws for its conduct in leaving the personal information of three million Massachusetts residents vulnerable to hackers, despite knowing for months that its website was insecure. Among other things, we allege that Equifax violated the Massachusetts Consumer Protection Act and Data Security Regulations, which require Equifax to develop, implement, and maintain reasonable administrative, technological, and physical safeguards to protect consumers' data from foreseeable harm. We also allege that Equifax failed to promptly notify consumers that their information was compromised, in violation of the Massachusetts Data Breach Notice Law, and that it compounded consumers' harm, including by charging consumers to implement security freezes necessitated by its own mistakes. In our view, Equifax could have prevented this breach, and it must be held accountable for failing to do so.⁵

The enforcement provisions contemplated by the Bill (Section 5) significantly infringe on this Office's enforcement powers to consumers' detriment. Although state Attorneys General have been the "cops on the beat" of the data security problem for the past decade,⁶ the Bill shifts primary enforcement authority from the States to the federal government. In our view, this would hamper the effectiveness of a federal law with respect to data breach notification and data security. Too many breaches occur for any one agency to respond effectively to all of them. Some breaches will be too small to be a priority at the federal level, yet such breaches could have a large impact in a particular state or region.

The Bill also erects procedural hurdles that further burden the States and infringe on their enforcement powers and prerogatives. 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 if the FTC initiates action first. It further allows the FTC to intervene in pending cases, and requires the consolidation of cases by different states into the U.S. District Court for the District of Columbia without regard to the locus of any of the parties. Such requirements inject delay and costs onto the States, unnecessarily complicating their enforcement efforts. Dual federal/state enforcement coordination of consumer protection laws

⁵ A copy of our Complaint is attached as **Exhibit 4**.

⁶ See generally, Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2017), available at <https://scholarship.law.nd.edu/ndlr/vol92/iss2/5>.

without such burdens is both possible and effective.⁷ To ensure meaningful protections for consumers, the Bill should likewise establish a dual federal/state enforcement framework that respects—not constricts—the enforcement prerogative and agility of the States.

Finally, we note with particular concern the provisions of this Bill that appear to foreclose the States’ ability to sue “financial institutions”—even in the face of the institution’s knowing failures to protect consumers’ data. *See* Section 5(b)(5). Our consumers rely on financial institutions to protect their most sensitive, personal information. An institution’s failure to implement reasonable data security safeguards to protect that information from a foreseeable breach represents a shocking betrayal of public trust, and poses an unacceptable risk to our consumers. This Bill prevents our Office, and all states, from discharging our duties to protect our consumers. There is no justification—especially in light of Equifax—for such a drastic rollback of the States’ enforcement powers.

II. The Bill Leaves Consumers in a Worse Position than the Status Quo.

a. The Bill’s Breach Notice Requirements (Section 4) Will Not Protect Consumers from Identity Theft, Financial Losses, or Other Harms.

If preventing identity theft and consumer harm is the goal of a data breach notice regime, requiring notice of the breach to the consumer as soon as possible must be the first priority. One study found that the breach of a Social Security number increases a consumer’s risk of identity theft by 18 times.⁸ Breaches of information such as email addresses, phone numbers, or other identifying information also subject the consumer to increased risks of scams, phishing, or other fraud. Prompt consumer notification allows consumers the opportunity take proactive steps to protect themselves from identity theft, financial fraud, or other harm before it occurs. Conversely, delayed notice increases the risk of harm by shortening or eliminating the window of opportunity for such prophylactic steps.

Public notice of a data breach also serves an important deterrent purpose. Having to notify customers of data security lapses creates a powerful incentive for a company to improve its data security practices to avoid a breach.

The consumer notification standards under this Bill (Section 4) do not achieve these goals. The Bill only requires consumer notice if the entity “determines after completion of [its] preliminary investigation ... that there is a reasonable risk that the breach ... *has resulted* in identity theft, fraud or economic loss...” *See* Section 4(b)(2). In other words, contrary to today’s regime under most state laws (where consumers are notified of breaches that raise the risks of *future* identity theft, fraud or economic loss), consumers would not be notified until *after that risk has manifested in harm*. This unacceptably externalizes the costs of a company’s poor

⁷ See, for example, the Federal Trade Commission Act (15 U.S.C. 45(a)(1) and its numerous state counterparts (*see, e.g.* Mass Gen. Laws c. 93A), and 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.*).

⁸ National Consumers League, *The Consumer Data Insecurity Report: examining the Data Breach – Identity Fraud Paradigm in Four Major Metropolitan Areas*, 14, (June 2014).

security practices onto consumers, an outcome especially unfair given that there is no clear authority to state Attorneys General to obtain restitution for such consumers. It also deprives the consumer of the ability to make his or her own determination of risk and take those steps he or she deems appropriate to mitigate it.

Further, by allowing the entity to determine whether or not consumers suffered harm before providing consumer notice, the Bill creates clear opportunities for abuse. Connecting any specific breach to identity theft or financial harm, or tracing identity theft to any particular breach over another, can be a difficult and time consuming process, and in practice, may be impossible. Because the Bill does not require the covered entity to conduct such an investigation,⁹ a covered entity might opt to avoid this expense. Finally, the Bill does not take into account non-financial harms that can occur from a data breach about which consumers should be notified, such as professional or personal embarrassment,¹⁰ or loss of access to online accounts or services.

Additionally, by requiring covered entities to conduct a preliminary investigation based on its own belief (reasonable or not) “that a breach of security containing personal information may have occurred,” without also imposing an outer time limit on that investigation risks injecting even further delay in the notification timeline. A federal standard should instead require breach notification as soon as reasonably practicable and without unreasonable delay when an entity knows, or has reason to know, that protected personal information of a consumer has been acquired without authorization, or used for unauthorized purposes.

Finally, the distinction drawn in the Bill between “covered entities” and “third parties” for purposes of notification (Section 4(c)) creates opportunities for delay as a result of disputes between covered entities as to which is the “third-party entity” and which is ultimately responsible for notice.¹¹ To ensure consumers are notified, Massachusetts imposes notification obligations based on the entity’s legal relationship to the breached personal information.¹²

⁹ Compare Section 4(a)(3) (requiring a covered entity to conduct a preliminary investigation based on its belief (reasonable or not) “that a breach of security containing personal information may have occurred,” to, among other things, “determine if the personal information has or is likely to have been acquired without authorization.”).

¹⁰ See Stipulated Order for Permanent Injunction and Other Equitable Relief, *FTC v. Ruby Corp., Ruby Life Inc., dba AshleyMadison.com, and ADL Media Inc.*, Case No. :16-cv-02438 (D.D.C. Dec. 14, 2016) (resolving FTC complaint alleging that operators of adult dating website had lax data security practices contrary to promises of privacy and security made to consumers, resulting in a data breach in August of 2015 and the publication by hackers of the sensitive profile, account security, and billing information for more than 36 million users).

¹¹ The Bill imposes the consumer notice obligation on “a covered entity” that “accesses, maintains, or stores personal, or handles personal information,” (Sections 2(7) and 4(b)(2)) but not on the “third party” entity that “processe[s], maintain[s], stores, or handles, or otherwise is permitted access to personal information in connection with providing services to a covered entity” (Section 2(1)(A)).

¹² See Mass Gen. Laws c. 93H, §§ 3(a), (b) (entities that “maintain or store, but do[] not own or license data” are obligated to promptly notify the owner or licensor, which are the entities that bear the ultimate duty to notify the consumers and state agencies).

b. The Bill Does Not Allow States to Adequately Redress Consumers' Losses.

Data breaches cause real harm to consumers. Armed with an individual's sensitive and personal information—including in particular a Social Security number, date of birth, and/or a drivers' license number—a criminal can commit identity theft, financial fraud, and other identity-related crimes. Identity theft results in real financial losses, loss of access to credit and even essential services like utilities, and fear and anxiety for consumers.¹³ Even if identity theft never occurs, victims of a data breach must spend time and money to protect themselves from future harm. Recommended measures include placing security freezes or fraud alerts, purchasing credit monitoring services, scrutinizing financial accounts and obtaining new account numbers, identification documents, or credentials, among other efforts.

Despite requiring entities to notify consumers only in circumstances where those consumers have suffered financial harm, the Bill does not authorize their state's Attorney General to obtain damages for that harm (and appears to preempt any state law, such as the Massachusetts Consumer Protection Act, that might allow for such a remedy). Rather, state Attorneys General would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information. As a result, and again, the Bill unacceptably passes the consequences of data breaches onto consumers. We urge the Committee not to preempt and displace the existing authority of state law enforcement to make their residents whole.

c. The Proposed "Security Safeguards" (Section 3) Should Be at Least as Strong as Existing Federal and State Standards.

The Subcommittee rightly recognizes that minimum data security standards are essential to protect consumers and businesses alike from data breaches. Indeed, our review of thousands of breach notifications underscores the importance of strong, and enforceable, data security standards. While some breaches result from intentional, criminal acts, many result from the failure to employ basic security practices, such as the improper disposal of consumers' information, lost files, disclosure through inadvertence, carelessness, or the failure to follow basic and well-accepted data security practices. Often even those breaches resulting from intentional criminal attacks could reasonably have been avoided or mitigated if the entity had complied with its own data security policies or employed basic security practices such as deploying software updates, patches, or firewalls.

Massachusetts has had robust minimum data security regulations in place since 2010 in the form of its Data Security Regulations (201 CMR 17.00 *et seq.*) and its Data Disposal Law (Mass Gen. Laws c. 93I). In our view, the flexible but strong minimum standards established by

¹³ In its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed. See U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft 2014*, at 6 & Table 6, available at <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>. The average out-of-pocket loss for those victims was \$2,895. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings." *Id.* at 8. With respect to consumers' emotional distress, the report also noted that more than one-third of identity theft victims were moderately or severely distressed due to the crime. See *id.* at 9, Table 9.

Massachusetts represent the leading, generally-applicable information security framework in the nation. Rather than employing a “one-size-fits-all” approach, Massachusetts utilizes a risk-based, process-oriented approach to data security, similar to well-established federal standards governing financial institutions and certain health-related entities.¹⁴

While Section 3 proposes a similar risk-based and flexible framework, it omits several key elements that, in our view, are necessary to ensure they are effective and enforceable. For example, both Massachusetts law and the FTC Safeguards Rule require entities to document their administrative, technical and physical safeguards, and update those policies as necessary.¹⁵ Such written information security programs are critical in ensuring that an entity develops, implements, and maintains a comprehensive and enforceable safeguards. The Subcommittee should also consider requiring entities that suffer a breach to document remedial actions and conduct post-incident reviews.

As to vendor management, the Bill is too lenient. Both the FTC Safeguards Rule and the Massachusetts Data Security Regulations require reasonable oversight of third party service providers. Massachusetts requires entities to “[o]versee 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 these regulations 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.” 201 CMR 17.03(2)(f). The FTC Safeguards Rule has a similar requirement. *See* 16 CFR § 314.4(d). By contrast, the Bill requires covered entities merely to “maintain reasonable procedures for the security of personal information by third parties” (Section 3(a)(3)(D)). In our experience, more robust third party oversight is necessary to prevent entities from outsourcing their responsibility to protect their customers’ data.

Finally, Section 3 does not define or enumerate any examples of the required “reasonable safeguards” that an entity must maintain, or provide any agency with rule-making authority to do so. For example, although the Bill generally contemplates that entities will maintain some form of computer and network system security, *see* Section 3(a)(3)(B)(ii), it does not specify what safeguards should be encompassed by that system. By contrast, both Massachusetts Law and the HIPAA Security Rule specify the various technical safeguards each requires, such as: secure

¹⁴ Massachusetts law requires covered entities to develop, implement, and maintain a written security program outlining administrative, technological, and physical safeguards appropriate for the entity’s size, scope of business, amount of resources available to it, the nature and quantity of data collected or stored, and the need for security of the personal information it handles. Within this flexible and technology-neutral framework, the regulations outline various categories of minimum security measures. *See generally*, **Exhibit 2** (201 CMR 17.00 *et seq.*). In this way, Massachusetts is similar to federal law governing financial institutions and health care information. *See* 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information) and 45 CFR Part 160 and Subparts A and C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information).

¹⁵ *See* 201 CMR 17.03(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...”); 16 CFR § 314.3(a) (“You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains the administrative, technical, and physical safeguards...”); 45 CFR § 164.316 (Policies and procedures and documentation requirements).

access control and user authentication procedures and mechanisms¹⁶; encryption of personal information sent over public networks or wirelessly, or stored on laptops and portable devices¹⁷; network security, such as up-to-date firewall protection and operating system security patches, and system security agent software¹⁸; and mechanisms to monitor computer systems for unauthorized use of or access to personal information.¹⁹

Forcing covered entities to guess what constitutes such “reasonable safeguards” exposes them to litigation risks, increases compliance uncertainty and costs, and may lead to a downward harmonization towards the least expensive (and likely least effective) measures. Relying on litigation to establish what is “reasonable” also will not keep pace with evolving security threats. For these reasons, we urge the Subcommittee to not override and preempt existing, more stringent state data security protection.

III. The Bill’s Proposed Preemption of State Law (Section 6) Will Prevent States from Protecting Their Consumers from Rapidly-Evolving Digital Risks.

Section 6 of the Bill would entirely and wrongly preempt existing state data breach and data security law that provide better protections for consumers. Federal standards should not preempt or undercut stronger provisions of state law, especially in the rapidly evolving space of cybersecurity and data protection. Instead of establishing a national security and breach standard that may fail to keep up with changing technologies, we urge the Subcommittee not to establish a ceiling for data security, but at most a federal “floor” of protections that state law can exceed as necessary to protect their consumers from emerging risks. *See, e.g.*, 15 U.S.C. § 6807(b) (Gramm-Leach-Bliley Act) (“[A] State statute, regulation, order, or interpretation is not inconsistent with this [law] if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this [law] . . .”).

Additionally, the scope of the proposed preemption is unduly broad, covering not only state laws concerning “personal information” but rather, state laws “with respect to securing *information* from unauthorized access or acquisition . . .” (emphasis added). This could sweep into its scope a multiple of existing state laws, such as state criminal laws concerning

¹⁶ *See, e.g.*, 201 CMR 17.04(1); 45 CFR §§ 164.308(a)(4), (5)(ii)(D); 164.312(a)(1), (2)(i).

¹⁷ *See e.g.*, 201 CMR 17.04(3), (5); 45 CFR § 164.312(a)(2)(iv), (e)(2)(ii).

¹⁸ *See, e.g.*, 201 CMR 17.04(6), (7).

¹⁹ *See, e.g.*, 201 CMR 17.04(4).

unauthorized access to a computer system²⁰ or the interception of wire communications,²¹ or laws protecting medical records and mental health records from unauthorized access.²²

Such a broad scope could further have a chilling effect on state legislatures, who are increasingly called on to respond to new and evolving security and privacy risks to their residents. In fact, this Office is actively engaged with the Massachusetts Legislature in order to bring additional tools and protections to consumers who are victims of data breaches.²³ The increasing threat and ever-evolving nature of data security risks demands the kind of agility and innovation that states are best positioned to provide. We urge the Subcommittee to respect the important role of the States and instead establish a minimum, not a maximum, standard of federal protection.

Conclusion

Thank you for this opportunity to convey our 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.

²⁰ See Mass. Gen. Laws c. 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.”).

²¹ See Mass. Gen. Laws c. 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”).

²² See, e.g., Mass Gen. Laws c. 111, § 70E(b), and c. 123, § 36.

²³ See S2304, *An Act Relative to Consumer Protection from Security Breaches* (<https://malegislature.gov/Bills/190/S2304>); H4241, *An Act Removing Fees for Security Freezes and Disclosures of Consumer Credit Reports* (<https://malegislature.gov/Bills/190/H4241>).

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

End of Document

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

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 in accordance with this chapter. 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. 93-110b) 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

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 § 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

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

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 17.05

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

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 § 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.

EXHIBIT 4

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

EQUIFAX, INC.

Defendant.

COMPLAINT

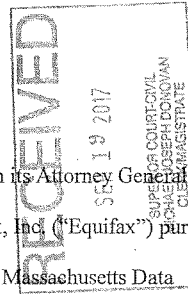
JURY TRIAL REQUESTED

INTRODUCTION

1. The Commonwealth of Massachusetts, by and through its Attorney General, Maura Healey ("Commonwealth"), brings this action against Equifax, Inc. ("Equifax") pursuant to the Massachusetts Consumer Protection Act (G.L. c. 93A) and the Massachusetts Data Security Law (G.L. c. 93H).

2. Equifax is one of three primary national credit-reporting bureaus in the United States. Equifax collects and maintains data regarding more than 820 million consumers worldwide, including at least 3,000,000 in Massachusetts. The personal data that Equifax holds touches upon virtually every aspect of a consumer's profile in the marketplace.

3. Equifax is a gatekeeper for consumers' access to socioeconomic opportunity and advancement. Every day, businesses across the country rely on Equifax's credit profiles to make decisions as to the credit worthiness of consumers. This information impacts many of the most important decisions in the lives of consumers—for instance, whether consumers can buy a house, obtain a loan, lease a vehicle, or even get a job.



4. Consumers do not choose to give their private information to Equifax, and they do not have any reasonable manner of preventing Equifax from collecting, processing, using, or disclosing it. Equifax largely controls how, when, and to whom the consumer data it stockpiles is disclosed. Likewise, consumers have no choice but to rely on Equifax to protect their most sensitive and personal data. Accordingly, it was and is incumbent on Equifax to implement and maintain the strongest safeguards to protect this data. Equifax has failed to do so.

5. From at least March 7, 2017 through July 30, 2017, a period of almost five months, Equifax left at least 143 million consumers' sensitive and private information exposed and vulnerable to intruders by relying on certain open-source code (called "Apache Struts") that it knew or should have known was insecure and subject to exploitation. Although patches, workarounds, and other fixes for the vulnerability were available and known to Equifax as of March 7, 2017, Equifax failed to avail itself of these remedies or employ other compensating security controls, such as encryption or multiple layers of security, that were sufficient to protect consumers' personal data.

6. As a result, intruders were able to access Equifax's computer system from at least May 13, 2017 through July 30, 2017, and potentially stole the sensitive and personal information of 143 million consumers (the "Data Breach"). The Data Breach, which Equifax first disclosed to the public on September 7, 2017, exposed to still-unknown persons some of the most sensitive and personal data of Massachusetts residents, including full names, social security numbers, dates of birth, addresses, and for some consumers, credit card numbers, driver's license numbers, and/or other unknown, personally-identifiable information.

7. Equifax could have—and should have—prevented the Data Breach had it implemented and maintained reasonable safeguards, consistent with representations made to the

public in its privacy policies, industry standards, and the requirements of Massachusetts law. Equifax did not do so.

8. By failing to secure consumer information, Equifax exposed over half of the adult population of Massachusetts to the risks of identity theft, tax return scams, financial fraud, health identity fraud, and other harm. Affected consumers have spent, and will continue to spend, money, time, and other resources attempting to protect against an increased risk of identity theft or fraud, including by placing security freezes over their credit files and monitoring their credit reports, financial accounts, health records, government benefit accounts, and any other account tied to or accessible with a social security number. The increased risk of identity theft and fraud as a result of the Data Breach also has caused Massachusetts consumers substantial fear and anxiety and likely will do so for many years to come.

9. Given the nature of Equifax's business, the sensitivity and volume of the data in which it traffics, and the serious consequences to consumers when that data is exposed, its failure to secure this information constitutes a shocking betrayal of public trust and an egregious violation of Massachusetts consumer protection and data privacy laws. As Equifax's own Chairman and Chief Executive Officer admitted, the Data Breach "strikes at the heart of who we are and what we do."

10. By this action the Commonwealth seeks to ensure that Equifax is held accountable, and not allowed to prioritize profits over the safety and privacy of consumers' sensitive and personal data. The Commonwealth seeks civil penalties, disgorgement of profits, restitution, costs, and attorney's fees, as available under G.L. c. 93A and G.L. c. 93H. The Commonwealth also seeks all necessary, appropriate, and available equitable and injunctive

relief to address, remedy, and prevent harm to Massachusetts residents resulting from Equifax's actions and inactions.

THE PARTIES

11. The Plaintiff is the Commonwealth of Massachusetts, represented by its Attorney General, who brings this action in the public interest pursuant to G.L. c. 93A, § 4, and G.L. c. 93H, § 6.

12. Defendant Equifax, Inc. is a publicly-traded Georgia corporation with its principal place of business at 1550 Peachtree Street N.E., Atlanta, Georgia.

JURISDICTION, AUTHORITY, AND VENUE

13. The Attorney General is authorized to bring this action, in this Court, under G.L. c. 93A, § 4, and G.L. c. 93H, § 6.

14. This Court has jurisdiction over the subject matter of this action by virtue of G.L. c. 93A, § 4, and G.L. c. 212, § 4.

15. This Court has personal jurisdiction over Equifax under G.L. c. 223A, § 3, including because Equifax has engaged in business with Massachusetts entities, and because Equifax's actions and inactions have affected Massachusetts residents.

16. Venue is proper in Suffolk County under G.L. c. 93A, § 4, as Equifax "has no place of business within the commonwealth," and under G.L. c. 223, § 5, as the Commonwealth is the plaintiff.

17. The Commonwealth notified Equifax of its intent to bring this action at least five days prior to the commencement of this action, as required by G.L. c. 93A, § 4.

FACTS*Equifax's Business*

18. Equifax's business centers on the collection, processing, and sale of information about people and businesses. According to its website, Equifax is a "global information solutions company" that "organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers." Equifax employs approximately 9,900 people worldwide.

19. As part of its business, Equifax creates, maintains, and sells "credit reports" and "credit scores" regarding individual consumers, including Massachusetts residents. Credit reports can contain, among other things, an individual's full social security number, current and prior addresses, age, employment history, detailed balance and repayment information for financial accounts, bankruptcies, judgments, liens, and other sensitive information. The credit score is a proprietary number, derived from a credit report and other information, that is intended to indicate relative to other persons whether a person would be likely to repay debts.

20. Third parties use credit reports and credit scores to make highly consequential decisions affecting Massachusetts consumers. For instance, credit scores and/or credit reports are used to determine whether an individual qualifies for a mortgage, car loan, student loan, credit card, or other form of consumer credit; whether a consumer qualifies for a certain bank account, insurance, cellular phone service, or cable or internet service; the individual's interest rate for the credit they are offered; the amount of insurance premiums; whether an individual can rent an apartment; and even whether an individual is offered a job.

The Data Breach

21. At all relevant times, Equifax maintained a publicly available website at www.equifax.com.

22. Within that website are various publicly available web pages directed to consumers, including Massachusetts residents. Among those web pages is one through which Equifax invites consumers to submit information to initiate and support a formal dispute of information in their credit reports (the "Dispute Portal").

23. Equifax maintained consumer names, addresses, full social security numbers, dates of birth, and for some consumers, driver's license numbers and/or credit card numbers of at least 143 million consumers, including nearly 3 million Massachusetts residents, in computer tables, databases, or files that were accessible (directly or indirectly) through the Dispute Portal (the "Exposed Information"). The Exposed Information, which included "Personal Information" as defined in G.L. c. 93H, § 1, and 201 CMR. 17.02, was not limited to the sensitive and personal information of those consumers who had used the Dispute Portal, but encompassed a larger group of consumers on whom Equifax held information.

24. Despite being accessible through a publicly available website, the Exposed Information was not "encrypted" on Equifax's systems as defined in 201 CMR 17.02.

25. Starting on or about May 13, 2017 through July 30, 2017, unauthorized third parties infiltrated Equifax's computer system via the Dispute Portal. Once in, the parties accessed and likely stole (i.e. "exfiltrated") the Exposed Information from Equifax's network.

*Equifax Ignored Numerous Signs that Its System
—and the Consumers’ Data Stored Therein—Was Vulnerable to Hackers*

26. According to a statement Equifax published online at <https://www.equifaxsecurity2017.com> on or about September 13, 2017, the Data Breach resulted when “criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638.”

27. Apache Struts is a piece of computer code used for creating web applications; i.e. a computer program that runs in a web browser.

28. At all relevant times, Equifax used Apache Struts, in whole or in part, to create, support, and/or operate its Dispute Portal.

29. As “open-source code,” Apache Struts is free and available for anyone to download, install, or integrate into their computer system. Apache Struts, like many other pieces of open-source code, comes with no warranties of any kind, including warranties about its security. Accordingly, it is incumbent on companies that use Apache Struts—like Equifax—to assess whether the open-source code is appropriate and sufficiently secure for the company’s purposes and that it is kept up-to-date and secure against known vulnerabilities.

30. There are, and at all relevant times have been, multiple well-known resources available to support companies relying on open-source code, including Apache Struts. These resources publicly announce to users when security vulnerabilities in the open-source code are discovered and verified, including in Apache Struts, compare the associated risks of such vulnerabilities, and propose fixes.

31. For example, the Apache Software Foundation (“Apache”), a non-profit corporation, releases updated versions of Apache Struts to “patch” it against verified security vulnerabilities. Apache also releases Security Bulletins on its website regarding security flaws in

Apache Struts, noting the nature of the vulnerability and ways to resolve it. Since 2007, Apache has posted at least 53 such security bulletins for Apache Struts.

32. Similarly, the U.S. Department of Commerce’s National Institute of Standards and Technology (“NIST”) maintains a free and publicly available National Vulnerability Database (“NVD”) at <http://nvd.nist.gov>. Using the NVD, NIST identifies security vulnerabilities, including in open-source code, the risks they pose, and ways to fix them, including as to security vulnerabilities in Apache Struts.

33. Likewise, the MITRE Corporation, a “not-for-profit organization that operates research and development centers sponsored by the [United States] federal government,”¹ also identifies code security vulnerabilities, including vulnerabilities in Apache Struts, using a Common Vulnerabilities and Exposures (“CVE”) Identifier. According to MITRE, the CVE Identifier is the industry standard for identifying publicly known cyber security vulnerabilities. MITRE maintains a database of CVE identifiers and the vulnerabilities to which they correspond, which is publicly accessible without cost online at <https://cve.mitre.org> (the “Vulnerability Database”).

34. On March 7, 2017, Apache published notice of a security vulnerability in certain versions of Apache Struts in its online security bulletins S2-045 and S2-046 (the “Apache Security Bulletins”). **Exhibit 1** (<https://cwiki.apache.org/confluence/display/WW/S2-045> last visited September 19, 2017) and **Exhibit 2** (<https://cwiki.apache.org/confluence/display/WW/S2-046> last visited September 19, 2017). The vulnerability was assigned the CVE identifier CVE-2017-5638 (the “March Security Vulnerability”).

¹ <https://www.mitre.org/>.

35. Directed to “All Struts2 developers and users,” the Apache Security Bulletins warned that the software was vulnerable to “Remote Code Execution,” or “RCE.” RCE refers to a method of hacking a public website whereby an online attacker can send computer code to the website that allows the attacker to infiltrate (that is, gain access to), and run commands on the website’s server (the computer that stores the information that supports the website).

36. The Apache Security Bulletins assigned the March Security Vulnerability a “maximum security rating” of “critical.” Apache recommended that users update the affected versions of Apache Struts to fix the vulnerability, or to implement other specific workarounds to avoid the vulnerability. **Exhibits 1 and 2.**

37. NIST also publicized the March Security Vulnerability in its NVD on or about March 10, 2017. **Exhibit 3** (<https://nvd.nist.gov/vuln/detail/CVE-2017-5638>, last visited September 19, 2017) (the “NIST Notice”). NIST noted that the severity of the vulnerability was an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System (“CVSS”). A score of 10.0 is the highest possible severity score on either scale. The NIST Notice also stated that an attack based on the vulnerability “[a]llows unauthorized disclosure of information,” would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password) to exploit the vulnerability. The NIST Notice also documented over twenty other website resources for advisories, solutions, and tools related to the March Security Vulnerability and how to patch or fix it.

38. Following the NIST Notice, the United States Computer Emergency Readiness Team (“US CERT”) issued a security Bulletin (Bulletin (SB17-079)) on March 20, 2017, calling out the March Security Vulnerability as a “High” severity vulnerability (“US CERT Alert”).

Exhibit 4 (excerpts from <https://www.us-cert.gov/ncas/bulletins/SB17-079>, last visited September 19, 2017) (relevant entry highlighted).

39. Likewise, MITRE included the March Security Vulnerability in the Vulnerability Database and documented various external website references to the March Security Vulnerability. **Exhibit 5** (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>, last visited September 19, 2017).

40. In the days following the public disclosure of the March Security Vulnerability by Apache, media reports claimed that hackers were exploiting the March Security Vulnerability against numerous companies, including banks, government agencies, internet companies, and other websites.

41. As Equifax disclosed on its website on or about September 13, 2017, the Data Breach occurred as a result of the exploitation of the March Security Vulnerability by hackers.

42. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that the March Security Vulnerability existed in Apache Struts.

43. Indeed, in a notice on the website <https://www.equifaxsecurity2017.com/>, Equifax stated that “Equifax’s Security organization was aware of this vulnerability” in Apache Struts in early March 2017.

44. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various

collateral sources referenced in the foregoing), that the implementation of Apache Struts it employed on its websites, including without limitation, the Dispute Portal was susceptible to the March Security Vulnerability.

45. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that it was vulnerable to unauthorized access to sensitive and personal consumer information by exploitation of the March Security Vulnerability by hackers.

46. Until at least July 30, 2017, and during the Data Breach, Equifax continued to use an Apache Struts-based web application that was susceptible to the March Security Vulnerability for its Dispute Portal.

47. Until at least July 30, 2017, and during the Data Breach, Equifax failed to employ successfully recommended fixes or workarounds, otherwise patch or harden its systems, or put in place any compensating controls sufficient to avoid the March Security Vulnerability, safeguard the Exposed Information, or prevent the Data Breach.

48. In addition, until at least July 29, 2017, and during the Data Breach, Equifax did not detect and/or appropriately respond to evidence that unauthorized parties were infiltrating its computer systems and had access to the Exposed Information; and/or did not detect or appropriately respond to evidence that those parties were exfiltrating the Exposed Information out of Equifax's computer system.

49. As a result of Equifax's actions and inactions, the Data Breach occurred, and hackers were able to access and likely stole the sensitive and personal data of 143 million consumers, including of Massachusetts consumers.

Equifax's Security Program Fell Short of Its Promises to Consumers and Massachusetts Law

50. At all relevant times, Equifax promised the public that safeguarding consumers' sensitive, personal information is "a top priority."

51. At all relevant times on its Privacy Policy, available through a hyperlink at the bottom of each page of its public website, Equifax represented to the public:

We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

52. Equifax likewise represented to consumers that it would keep all of their credit information, including that which consumers submitted through the Dispute Portal, secure. In its "Consumer Privacy Policy for Personal Credit Reports," accessible at <http://www.equifax.com/privacy/personal-credit-reports>, Equifax represented that it has "reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers'] personal information."

53. By failing to patch or otherwise address the March Security Vulnerability, detect the hackers in their network, prevent them from accessing and stealing the Exposed Information, and otherwise failing to safeguard the Exposed Information, as set forth in paragraphs 21 to 49 herein, Equifax failed to live up to its representations to the public.

54. Equifax also failed to comply with Massachusetts Law.

55. The Massachusetts Data Security Regulations, promulgated pursuant to G.L. c. 93H, § 2(a), went into effect on March 1, 2010. The objectives of the Data Security Regulations are 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.” G.L. c. 93H, § 2(a).

56. The Data Security Regulations “establish minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.” 201 CMR 17.01(1). These minimum standards include, among others, the development, implementation, and maintenance of a comprehensive written information security program (a “WISP”) that contains enumerated, minimum safeguards to secure personal information owned or licensed by the entity. See 201 CMR 17.03.

57. The Data Security Regulations also require that an entity “establish[] and maint[ain] . . . a security system covering its computers” that contains certain minimum enumerated safeguards to prevent security compromises. See 201 CMR 17.04.

58. By failing to patch or otherwise sufficiently address the March Security Vulnerability, detect and appropriately respond to the presence of unauthorized parties in its network, prevent those parties from accessing and/or stealing the Exposed Information, and/or safeguard the Exposed Information, as set forth in paragraphs 21 to 49 herein, Equifax failed to develop, implement, or maintain a WISP that met the minimum requirements of the Data Security Regulations, 201 CMR 17.03 and 17.04.

59. In addition, the Data Security Regulations required Equifax to go beyond these minimum requirements and develop, implement, or maintain in its WISP additional safeguards that were “appropriate to” the “size, scope and type of business” of Equifax, the “amount of resources available to [it],” the “amount of stored data,” and “the need for security and confidentiality of both consumer and employee information.” 201 CMR 17.03(1).

60. Equifax is a large, sophisticated, multinational company of nearly 10,000 employees and billions of dollars in annual revenue whose primary business consists of acquiring, compiling, analyzing, and selling sensitive and personal data. Equifax holds the personal information and other personal data of more than 820 million consumers internationally—more than twice the population of the United States. This includes information that is sought after by hackers because it can be used to commit identity theft and financial fraud. As such, the Data Security Regulations required Equifax to implement administrative, technical, and physical safeguards that substantially exceed the minimum standards set forth in the Data Security Regulations, and which are at least consistent with industry best practices.

61. For example, and without limitation, Equifax’s size, scope and type of business, the amount of resources available to it, the amount of stored data, and the need for security and confidentiality of both consumer and employee information made it “appropriate” and necessary under the Data Security Rules for Equifax to have encrypted any Personal Information that was accessible via the publicly accessible, and vulnerable, Dispute Portal. It was also “appropriate” and necessary for Equifax to have maintained multiple layers of security sufficient to protect personal information stored in its system should other safeguards fail. By failing to do so, Equifax failed to comply with 201 CMR 17.03(1).

Equifax Delayed Notifying the Public of the Data Breach

62. Chapter 93H requires covered entities to report data breaches to the Commonwealth, including the Attorney General's Office and the Office of Consumer Affairs and Business Regulation, "as soon as practicable and without unreasonable delay, when such person . . . (1) knows or has reason to know of a breach of security [as that term is defined in G.L. c. 93H, § 1(a)], 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[.]" G.L. c. 93H, § 3(b).

63. As of or soon after July 29, 2017, Equifax knew or should have known that the "personal information" (as defined in G.L. c. 93H, § 1(a)) of at least one Massachusetts resident was acquired by an unauthorized person, and/or of a "breach of security," and that it thus had a duty to provide notice to the Attorney General's Office and the Office of Consumer Affairs and Business Regulation under chapter 93H, § 3(b) "as soon as reasonably practicable and without unreasonable delay."

64. Equifax delayed providing notice to the Attorney General or the Office of Consumer Affairs and Business Regulation until September 7, 2017. Equifax thus failed to provide timely notice under chapter 93H, § 3(b).

65. Chapter 93H, § 3(b) also requires an entity to provide timely written notice, with content specified by § 3(b), of a reportable data breach to each affected consumer. Such notice, when promptly given, allows the consumer to take steps to protect him or herself from identity theft, fraud, or other harm that may result from the breach.

66. Under chapter 93H, § 1, a breached entity may provide "substitute notice" to consumers "if the person . . . 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 . . . does not have sufficient contact information to provide notice.” Substitute notice consists of all three of the following: (1) email notice to the extent the entity has email addresses for the affected residents, (2) a “clear and conspicuous posting of the notice on the home page” of the notifying entity and (3) “publication in or broadcast through media or medium that provides notice throughout the commonwealth.” G.L. c. 93H, §1.

67. Equifax knew or should have known as of or soon after July 29, 2017, that it met the threshold for being able to provide “substitute notice” as defined in chapter 93H, § 1.

68. Despite this, Equifax did not then avail itself of any element of the substitute notice process but instead delayed notifying the public of the Data Breach for nearly six weeks, until September 7, 2017, through a website posting. Equifax thus failed to provide timely notice to affected consumers as required by chapter 93H, § 3(b).

Equifax’s Actions and Inactions in Connection with the Data Breach Have Created, Compounded, and Exacerbated the Harms Suffered by the Public

69. The Attorney General is not required to demonstrate harm to consumers in order to enforce the Data Breach Notice Law (G.L. c. 93H), the Data Security Regulations (201 CMR 17.00–17.05), or the Consumer Protection Act (G.L. c. 93A).

70. Nevertheless, consumers clearly have already suffered significant and lasting harm as a result of the Data Breach, and such harm is likely to continue and worsen over time.

71. Armed with an individual's sensitive and personal information—including in particular a social security number, date of birth, and/or a drivers' license number—a criminal can commit identity theft, financial fraud, and other identity-related crimes. According to the Federal Trade Commission ("FTC"):

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.²

72. Identity theft results in real financial losses, lost time, and aggravation to consumers. In its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed.³ The average out-of-pocket loss for those victims was \$2,895. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."⁴ With respect to consumers' emotional distress, the report also noted that more than one-third of identity theft victims were moderately or severely distressed due to the crime.⁵

73. The Data Breach has substantially increased the risk that the affected Massachusetts consumers will be a victim of identity theft or financial fraud at some unknown point in the future.

² See <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft>.

³ U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft 2014, at 6 & Table 6, available at <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>.

⁴ Id. at 8.

⁵ See id. at 9, Table 9.

74. In order to protect themselves from this increased risk of identity theft and fraud, many consumers may place “security freezes” on their credit reports with one or more consumer reporting agency, including Equifax. The primary objective of a security freeze is to prevent third parties from accessing the frozen credit report when a new application for credit is placed without the consumer’s consent.

75. Massachusetts law permits, but does not require, the consumer reporting agency to charge the consumer a “reasonable fee, not to exceed \$5,” to place, lift, or remove a freeze on the consumer’s credit report. See G.L. c. 93, § 62A.

76. As a result of Equifax’s actions and inactions in connection with the Data Breach, and in an effort to protect themselves against identity theft or financial fraud, many Massachusetts consumers have already spent and will continue to spend time and money in an effort to place security freezes on their credit reports with Equifax and other consumer reporting agencies.

77. Further, Equifax has complicated consumers’ efforts to protect themselves from the harms caused by the Data Breach by failing to take various measures that it was uniquely positioned to take to mitigate the risk of harm caused by the Data Breach. Instead, Equifax has failed to clearly and promptly notify consumers whether they were affected by the Data Breach, has charged consumers to place security freezes (and presumably unfairly profited thereby), has failed to offer consumers free credit and fraud monitoring beyond one year, and has failed to ensure adequate call center staffing and availability of online services in the days following the September 7, 2017 announcement of the Data Breach. Equifax’s actions and inactions in this regard have compounded the harms already suffered by consumers.

CAUSES OF ACTION

COUNT I

Violations of G.L. c. 93H, § 3 – Failure to Give Prompt Notice of Data Breach

78. The Commonwealth incorporates and realleges herein the allegations in paragraphs 1–77.

79. The Commonwealth “may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate.” G.L. c. 93H, § 6.

80. As a corporation, Equifax is a “person” under G.L. c. 93H, § 1(a).

81. General Laws c. 93H, § 3(b) requires that a person who:

[O]wns 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.

82. “Personal Information” is defined in G.L. c. 93H, § 1(a) as:

[A] [Massachusetts] 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

83. At all relevant times, Equifax owned or licensed personal information of at least one Massachusetts resident, as the term “personal information” is defined in G.L. c. 93H, § 1(a).

84. As of or soon after July 29, 2017, Equifax knew or should have known that the “personal information” (as defined in G.L. c. 93H, § 1(a)) of at least one Massachusetts resident

was acquired by an unauthorized person, and/or that the Data Breach was a “breach of security” as defined in G.L. c. 93H, § 1(a).

85. As of or soon after July 29, 2017, Equifax knew or should have known that it met the threshold for being able to provide “substitute notice” to Massachusetts residents as defined in G.L. 93H, § 1(a).

86. Equifax did not provide notice to the Attorney General, the Office of Consumer Affairs and Business Regulation, and affected consumers until September 7, 2017.

87. By not providing notice, substitute or otherwise, “as soon as practicable and without unreasonable delay” to the Attorney General, the Office of Consumer Affairs and Business Regulation, and affected consumers, Equifax violated G.L. c. 93H, § 3(b).

88. Each failure to notify each affected Massachusetts consumer, the Attorney General, and the Office of Consumer Affairs and Business Regulation constitutes a separate violation of G.L. c. 93H.

COUNT II

**Violations of G.L. c. 93H/201 CMR 17.00–17.05 –
Failure to Safeguard Personal Information**

89. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–88.

90. The Commonwealth “may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate.” G.L. c. 93H, § 6.

91. The Data Security Regulations, 201 CMR 17.00-17.05, were promulgated under authority of G.L. c. 93H, § 2.

92. The Data Security Regulations “apply to all persons that own or license personal information about a resident of the Commonwealth.” 201 CMR 17.01(2).

93. As a corporation, Equifax is a “person” under the Data Security Regulations. See 201 CMR 17.02.

94. The definition of “Personal Information” in the Data Security Regulations is coextensive to the definition of “Personal Information” in G.L. c. 93H, § 1, which is set forth in paragraph 82. See 201 CMR 17.02.

95. An entity “owns or licenses” personal information under the Data Security Regulations if it “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.” 201 CMR 17.02.

96. Equifax is bound by the Data Security Regulations because at all relevant times, it owned or licensed personal information of at least one Massachusetts resident and continues to own or license the personal information of Massachusetts residents.

97. The Data Security Regulations “establish[] minimum standards to be met in the connection with the safeguarding of personal information contained in both paper and electronic records.” 201 CMR 17.01(1).

98. Among these minimum standards is the duty of “[e]very person that owns or licenses personal information about a resident of the Commonwealth” to “develop, implement, and maintain” a written information security program (a “WISP”) that “contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business . . . ; (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.” 201 CMR 17.03(1).

99. The Data Security Regulations mandate certain minimum safeguards and obligations that an entity must develop, implement, and maintain in its WISP, including among others:

- To “[i]dentify[] and assess[] reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic . . . records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks[.]” (201 CMR 17.03(2)(b));
- “[M]eans for detecting and preventing security system failures.” (201 CMR 17.03(2)(b)(3)); and
- “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.” (201 CMR 17.03(2)(h)).

100. The WISP must also include the “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,” contains certain minimum elements, including:

- “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[.]” (201 CMR 17.04(1));
- “[S]ecure access control measures” over computer systems that “restrict access to records and files containing personal information to those who need such information to perform their job duties” (201 CMR 17.04(2)(a));
- “[S]ecure access control measures” over computer systems that “(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[.]” (201 CMR 17.04(2)(b));

- “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.” (201 CMR 17.04(3));
- “Reasonable monitoring of systems, for unauthorized use of or access to personal information[.]” (201 CMR 17.04(4));
- “For files containing personal information on a system that is connected to the Internet, . . . reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information[.]” (201 CMR 17.04(6)); and
- “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.” (201 CMR 17.04(7)).

101. Equifax failed to develop, implement, and maintain its WISP and a security system covering its computers in such a way as to meet the minimum requirements of 201 CMR 17.03 and 201 CMR 17.04, including without limitation the minimum requirements set forth in 201 CMR 17.03(2)(b), (2)(b)(3), or (2)(h)); or 201 CMR 17.04(1), (2)(a), (2)(b), (3), (4), (6), or (7).

102. Equifax also failed to satisfy its obligations to develop, implement, and maintain a WISP that contained “administrative, technical, and physical safeguards that are appropriate” to: (a) “the size, scope and type of business of” Equifax; (b) “the amount of resources available to” Equifax; (c) the amount of data Equifax stores; and (d) “the need for security and confidentiality of both consumer and employee information.” 201 CMR 17.03(1).

103. These failures include, without limitation: not adequately patching or implementing other safeguards sufficient to avoid the March Security Vulnerability; keeping the Exposed Information unencrypted or otherwise not protected through other methods from unauthorized disclosure in an area of its network accessible to the Internet; and not maintaining multiple layers of security sufficient to protect personal information from compromise.

104. Each violation of the Data Security Regulations as to each affected Massachusetts resident is a separate violation of c. 93H, § 2.

105. Accordingly, Equifax violated G.L. c. 93H, § 2.

COUNT III

Violations of G.L. c. 93A, § 2 – Unfair Acts or Practices

106. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–105.

107. General Laws c. 93A, § 2(a) declares unlawful “unfair or deceptive acts or practices in the conduct of trade or commerce[.]”

108. Equifax conducts trade and commerce in Massachusetts and with Massachusetts consumers.

109. As a corporation, Equifax is a “person” under G.L. c. 93A, § 1(a).

110. Equifax has engaged in unfair or deceptive acts or practices in violation of G.L. c. 93A § 2(a).

111. Equifax’s unfair or deceptive acts or practices include: (a) failing to promptly notify the public (including the Attorney General’s Office and affected residents) of the Data Breach despite the existence of substantial risk to consumers from the Data Breach; and/or (b) failing to maintain reasonable safeguards sufficient to secure the private and sensitive information about Massachusetts consumers from known and foreseeable threats of unauthorized access or unauthorized use, including identity theft, financial fraud, or other harms.

112. In addition, each of Equifax's violations of G.L. c. 93H and 201 CMR 17.00–17.05, as alleged herein and in Counts I & II, *supra*, are unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2(a).

113. Accordingly, Equifax violated G.L. c. 93A, § 2.

114. Each and every violation of G.L. c. 93H and 201 CMR 17.00–17.05 with respect to each Massachusetts consumer is a separate violation of G.L. c. 93A, § 2.

115. Equifax knew or should have known that each of its violations of G.L. c. 93H and 201 CMR 17.00–17.05, each failure to maintain reasonable safeguards to protect Massachusetts consumers' sensitive and personal information, and each failure to promptly notify the public of the Data Breach, would violate G.L. c. 93A, § 2.

116. Although consumer harm is not an element of a claim under c. 93A, § 4, each and every consumer affected by the Data Breach has suffered and/or will suffer financial losses, and the associated stress and anxiety, as a result of the above unfair or deceptive acts or practices, including without limitation the costs to place, lift, and/or terminate security freezes with all applicable consumer reporting bureaus, remedial measures to prevent or respond to identity theft or other fraud, and out of pocket losses resulting therefrom.

COUNT IV

Violation of G.L. c. 93A, § 2 – Deceptive Acts or Practices

117. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–116.

118. At all relevant times, Equifax represented to the public on its online Privacy

Policy that it has:

[B]uilt our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

119. In its “Consumer Privacy Policy for Personal Credit Reports,” accessible at <http://www.equifax.com/privacy/personal-credit-reports>, Equifax further publicly represented that it has “reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers’] personal information.”

120. Equifax’s failures: to patch or otherwise adequately address the March Security Vulnerability; detect the hackers in their network; prevent them from accessing and stealing the Exposed Information; and otherwise failing to safeguard the Exposed Information, as alleged in paragraphs 21 to 49, herein, rendered these representations deceptive.

121. Additionally, Equifax’s failure to implement, develop, and/or maintain a WISP compliant with the Data Security Regulations or industry standards, as alleged in paragraphs 50 to 61 and 89 to 105, herein, rendered these representations deceptive.

122. Equifax’s public representations of the nature of its security safeguards over Massachusetts consumers’ sensitive and personal information were unfair or deceptive under G.L. c. 93A, § 2(a).

123. Accordingly, Equifax violated G.L. c. 93A, § 2.

124. Equifax knew or should have known that its misrepresentations of the nature of its security safeguards over Massachusetts consumers’ sensitive and personal information would violate G.L. c. 93A, § 2.

COUNT V

Violation of G.L. c. 93A , § 2 – Unfair or Deceptive Trade Practices

125. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1– 124.

126. Equifax committed unfair or deceptive acts or practices under G.L. c. 93A, § 2, by failing to adequately allow or otherwise hindering the ability of Massachusetts consumers to protect themselves from harm resulting from the Data Breach by failing to make sufficiently available measures that Equifax was uniquely positioned to provide to mitigate the public harm caused by the Data Breach, namely:

- Timely notice of the Data Breach;
- Free security freezes of Equifax credit reports;
- Free Credit and fraud monitoring of Equifax credit reports for more than one year;
- Ensuring adequate and competent call center staffing related to the Data Breach;
- and
- Ensuring the availability of online services that notified consumers of whether they were affected by the Data Breach and allowed consumers to place a security freeze.

127. Accordingly, Equifax violated G.L. c. 93A, § 2.

128. Equifax knew or should have known that that the conduct described in paragraphs 69 to 77and 125 to 126 would violate G.L. c. 93A, § 2.

PRAYER FOR RELIEF

WHEREFORE, the Commonwealth requests that the Court grant the following relief:

1. Enter a permanent injunction prescribing appropriate relief;
2. Order that Equifax pay civil penalties, restitution, and costs of investigation and litigation of this matter, including reasonable attorney's fees, to the Commonwealth of Massachusetts as provided for under G.L. c. 93A, § 4, in an amount to be determined at trial;
3. Disgorge profits Equifax obtained during or as a result of the Data Breach; and
4. Order such other just and proper legal and equitable relief.

REQUEST FOR JURY TRIAL

The Commonwealth hereby requests trial by jury as to all issues so triable.

Respectfully submitted,

COMMONWEALTH OF MASSACHUSETTS

MAURA HEALEY
ATTORNEY GENERAL

By: 

Sara Cable (BBO #667084)
Jared Rinehimer (BBO #684701)
Michael Lecaroz (BBO #672397)
Assistant Attorneys General
Consumer Protection Division
One Ashburton Place, 18th Floor
Boston, MA 02108
(617) 727-2200
sara.cable@state.ma.us
jared.rinehimer@state.ma.us
michael.lecaroz@state.ma.us

Date: *September 19, 2017*



Statement of Francis Creighton
President & CEO
Consumer Data Industry Association

Before the
Subcommittee on Financial Institutions & Consumer Credit
Committee on Financial Services
United States House of Representatives

Hearing on
“Legislative Proposals to Reform the Current Data Security
and Breach Notification Regulatory Regime”

March 7, 2018

Chairman Luetkemeyer, Ranking Member Clay, and Members of the Subcommittee, thank you for the opportunity to appear before you.

My name is Francis Creighton, and I am President & CEO of the Consumer Data Industry Association. CDIA is a trade association representing more than 100 corporate members, including the three nationwide credit bureaus – Equifax, Experian and Transunion. Our other members include specialty credit bureaus, resellers and the largest background screening companies. We educate policymakers, regulators, consumers and others on how the responsible use of consumer data empowers economic opportunity.

You have asked me to testify about two legislative proposals: the "Data Acquisition and Technology Accountability and Security Act," and H.R. 4028, the "PROTECT Act of 2017," including any suggestions to improve these legislative proposals. More generally, you have asked me to "address opportunities to reform current federal and state data security regulatory regimes in order to close any gaps in data security and data breach regulation, as well as reduce vulnerabilities or shortcomings in the current regulatory regime." I will endeavor to address these issues, but first would like to provide some context for what the consumer reporting industry does and how we are regulated.

Consumers today benefit from a democratic, accurate and fair credit system. Individual consumers have the liberty to access credit anywhere in the country from a wide variety of lenders based solely on their own personal history of handling credit. Families buying a home

for the first-time access mortgage products that suit their individual needs and capabilities. Young people who have new jobs in a new city can go to an auto dealer and drive away with a financed car even without any history in that community. With the rise of the internet, new credit opportunities have expanded even further to meet individual needs.

If a consumer has been a responsible user of credit in the past, lenders and others are more likely to offer credit at the most favorable terms – terms that previously were reserved for the wealthy. Credit reporting companies and other CDIA members are helping solve the problem of the unbanked and credit invisible populations by expanding the kinds of data we collect, giving lenders and others information that allow more consumers to responsibly access traditional financial services and integrate consumers into the mainstream financial system.

Most consumers pay their bills on time, and are rewarded for doing so when they seek out new credit and their report shows a positive history. Without the credit reporting system, lenders would have no way to judge whether an individual applying for credit has previously paid their bills or not. Lenders and other users of credit reports would find it difficult to assess risk in the larger population if credit files were missing important information. The safe and sound choice for a lender would be to raise interest rates on loan products to account for greater risk, with the consumer who has been consistently making the right choices losing out.

Credit reports are also important in helping consumers who may not have stellar credit avoid getting shut-out from the credit system altogether. Specifically, “risk based pricing” enables

consumers who may be more of a risk based on their credit payment history to still have access to credit. A broad-based credit reporting system enables lenders to compete, enabling more consumers to get more credit choices and at lower rates as lenders compete for consumers' business.

In creating, amending and affirming the Fair Credit Reporting Act since 1970, Congress has weighed the competing priorities of safety and soundness, privacy, accuracy, security and economic benefits. The result is a detailed regulatory regime limiting the sharing of information for defined permissible purposes only and strict requirements on accuracy, consumer access and correction. Our consumer reporting system protects privacy and ensures that banks have a clear picture of the risk associated with lending to a particular consumer, all of which leads to the most efficient, fair and cost-effective credit system in the world.

Our credit reports tell the story of our individual choices. They are neither positive nor negative; they are simply the best attempt at an accurate portrait of what we have done, and they give lenders and others the tools they need to assess how a particular person will handle her or his obligations in the future. Because credit reports are constantly updated with new information, a single missed payment, for example, is set in the context of years of on-time payments. Our credit reporting system allows for second chances for American consumers.

Other countries are actively working to emulate our credit system, working with the World Bank¹ and others to bring the kinds of opportunities we have here to the rest of the world. Our credit reporting system is a main reason American consumers have a diverse range of lenders and products from which to choose, in stark contrast to many other financial systems, even those in developed nations.

Credit reports also give a variety of different kinds of lenders access to the same kind of information, giving a local community bank or credit union a chance to compete against a trillion-dollar financial institution. As Richard Cordray, former Director of the Consumer Financial Protection Bureau (CFPB), said in 2012 at a Field Hearing:

“Without credit reporting, consumers would not be able to get credit except from those who have already had direct experience with them, for example from local merchants who know whether or not they regularly pay their bills. This was the case fifty or a hundred years ago with “store credit,” or when consumers really only had the option of going to their local bank. But now, consumers can instantly access credit because lenders everywhere can look to credit scores to provide a uniform benchmark for assessing risk.”²

Credit reports also check human bias and assumptions, providing lenders with facts that contribute to equitable treatment for consumers. CDIA members establish an accountable and colorblind system for judging creditworthiness designed both for the best interests of

¹ See e.g. World Bank. General principles for credit reporting (September 1, 2011) (accessed February 21, 2018), <http://www.worldbank.org/en/topic/financialsector/publication/general-principles-for-credit-reporting>

² Cordray, Richard. Prepared Remarks by Richard Cordray on Credit Reporting (July 16, 2012) (accessed February 22, 2018), <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-by-richard-cordray-on-credit-reporting/>.

consumers and safety and soundness of lending institutions. Without this system, subjective judgements could be based on factors other than the facts of creditworthiness.

This Committee has been at the forefront of ensuring that lenders are making responsible choices, especially in the wake of the 2008 financial crisis. CDIA members provide businesses with the information and analytical tools necessary to manage risk and protect consumers. Federal regulators require lenders and others, such as Fannie Mae and Freddie Mac, to use credit reports to assess the creditworthiness of prospective borrowers. The proliferation of “NINJA” (No Income, No Job or Assets) loans in the last decade’s mortgage market, when some lenders pulled credit reports but effectively ignored them in return for higher rates, illustrates the importance of using credit reports to protect the financial system³.

Current Law Data Security Requirements for Credit Reporting Companies

Since September of last year, increased attention has been paid to how national CRAs secure credit file information and how that security is regulated. The industry is currently highly regulated, by the states, federal regulators, laws, contracts and other obligations.

³ NINJA lenders operated in a variety of ways – some depended on credit reports, but ignored other aspects of the loan file, such as income or employment status. While there were legitimate reasons for offering some of these loans, the record shows that traditional lending standards were put aside in an effort to maximize the number of loans closed.

The Gramm-Leach-Bliley Act & FTC Safeguards Rule

Credit reporting agencies are recognized as financial institutions subject to the information security requirements of the Gramm-Leach-Bliley Act (GLBA), and its implementing regulation, the Standards for Safeguarding Customer Information (“Safeguards Rule”) promulgated by the Federal Trade Commission (FTC)⁴. The Safeguards Rule imposes specific standards designed to:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of such records; and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer⁵.

The Safeguards Rule requires financial institutions to “develop, implement, and maintain a comprehensive information security program” that includes appropriate administrative, technical and physical safeguards to achieve these objectives. This program is required to be tailored to the institution’s size and complexity, the nature and scope of its activities and the sensitivity of customer information⁶.

⁴ 15 U.S.C. § 6801; 16 C.F.R. pt. 314. The Safeguards Rule applies to financial institutions within the FTC’s jurisdiction, which includes credit reporting companies. The federal prudential banking regulators (Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation) have promulgated similar information security guidance that applies to the financial institutions under their supervision. See Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, App. B (interagency guidelines as promulgated by the OCC); 12 C.F.R. pt. 208, App. D-2 (as promulgated by the Federal Reserve); 12 C.F.R. pt. 364, App. B (as promulgated by the FDIC).

⁵ 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).

⁶ 16 C.F.R. § 314.3(a).

Financial institutions, including credit reporting agencies, must also designate an employee to coordinate their comprehensive information security program, as well as identify reasonably foreseeable risks to the security of the information. Financial institutions must assess the sufficiency of safeguards and design, implement and regularly test safeguards to protect against such risks⁷. Finally, the Safeguards Rule obligates financial institutions to oversee their service providers' cybersecurity practices, both by taking reasonable steps to ensure their service providers employ strong security practices, and by entering into contracts with such providers that require them to implement appropriate safeguards⁸.

These are general parameters designed to keep pace with evolving threats. Regulators anticipated that private institutions and their direct regulators and supervisors would fine-tune industry best practices over time.

The Federal Trade Commission Act (FTC Act)

Credit reporting companies are also subject to the FTC's jurisdiction over cybersecurity matters under Section 5 of the FTC Act⁹. Under this law the FTC is empowered to take action against any business that engages in "unfair or deceptive acts or practices" ("UDAP"), which the agency has interpreted to include inadequate data security practices¹⁰.

⁷ 16 C.F.R. § 314.4.

⁸ 16 C.F.R. § 314.4(d).

⁹ 15 U.S.C. § 45.

¹⁰ See Congressional Research Service, "The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority" (September 11, 2014) (accessed February 22, 2018), <https://fas.org/sgp/crs/misc/R43723.pdf>.

The FTC requires companies to employ safeguards for information that are “reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities¹¹.” While specific cybersecurity requirements under Section 5 are not codified, the FTC has issued detailed guidance that explains what it considers to be reasonable cybersecurity safeguards. These include practices such as encryption, use of firewalls, use of breach detection systems, maintaining physical security of objects that contain sensitive information and training employees to protect such information¹².

In addition to issuing detailed guidance, the FTC zealously enforces these standards, having brought over 60 cases since 2002 against businesses for putting consumer data at “unreasonable risk¹³.” It is our understanding, for example, that the FTC is the lead agency investigating the Equifax data breach.

The Fair Credit Reporting Act

When credit reporting first began, there was little standardization in the methods used and types of information collected as it was a decentralized, city-by-city, industry. In particular, there was no standard procedure for consumers to find out what was in a credit report and to

¹¹ Federal Trade Commission, “Data Security” (accessed February 22, 2018), <https://www.ftc.gov/datasecurity>.

¹² See, e.g., Federal Trade Commission, “Protecting Personal Information: A Guide for Business” (accessed February 28, 2018), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹³ See Federal Trade Commission, “Privacy and Data Security Update (2016)” (January 2017) (accessed February 22, 2018), <https://www.ftc.gov/reports/privacy-data-security-update-2016>.

have erroneous information corrected. In response to these concerns, the first voluntary standards of practice were pioneered by the industry in the 1960s and these later served as the basis for many provisions in the first Fair Credit Reporting Act (FCRA). The FCRA imposed duties on credit reporting companies (referred to as “consumer reporting agencies” under the statute), which included requiring lenders and other users of credit reports to notify consumers when they take “adverse action” based on a credit report, requiring the agencies to disclose all information in the credit file to consumers upon request and providing for a mechanism for consumers to dispute and correct inaccurate or incomplete information.

Building on the core structure of the FCRA, Congress revised the law in 1996. One of the most important revisions was to impose a set of duties, not just on the credit reporting companies themselves but on businesses that furnish information to the credit bureaus in the first place. In 2003, again building on the FCRA’s core structure, Congress, led by this Committee, further modified the FCRA by passing the Fair and Accurate Credit Transactions Act, which allowed consumers to receive free credit reports annually and included important new protections for identity theft victims¹⁴, many of which built on industry-set practices already in place at that time.

Under the FCRA, credit reporting companies are subject to a comprehensive regulatory regime of consumer protections. A number of these provisions are designed to protect consumer privacy, such as the aforementioned permissible purpose and credentialing requirements. The

¹⁴ FCRA § 609(e).

FCRA also includes criminal penalties for people who obtain credit reports under false pretenses or credit reporting companies that knowingly provide credit reports to persons not authorized to receive them, for example, by selling consumers' private information to a litigation opponent or an ex-spouse hoping to find embarrassing information¹⁵.

The FCRA also addresses the accuracy and completeness of consumer reports. The most basic of these protections is the consumer's right to know what is in the credit file¹⁶. The 2003 amendments to the FCRA additionally required credit bureaus to provide consumers with free annual disclosures of the information in the file, including through an official website, www.annualcreditreport.com, for the nationwide bureaus. Further, when a user of a consumer report takes "adverse action" against a consumer on the basis of information in the credit report, that user must provide the consumer with a notice that contains information about how the consumer can obtain a copy of the credit report and can get errors corrected¹⁷. For example, if a lender denies a consumer's application because of a low credit score the lender must provide the consumer with a notice of adverse action. This notice enables consumers to understand that there may be adverse information in their credit file, and encourages the consumer to obtain a free copy of their credit report to examine it for possible errors.

¹⁵ FCRA § 607(a).

¹⁶ FCRA § 609.

¹⁷ FCRA § 615(a).

In addition, consumers have the right to dispute information in the file, and the credit reporting company is obligated to conduct a reasonable investigation of the dispute¹⁸. Credit reporting companies must also independently employ reasonable procedures to assure maximum possible accuracy of the information in consumer files¹⁹.

The FCRA also requires that credit reporting companies only provide credit reports to legitimate companies or people with a “permissible purpose” to receive such reports, such as credit or insurance underwriting. Companies’ procedures must require that prospective users of credit reports identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. The FTC has brought multiple actions over the years seeking to enforce these provisions, most notably against ChoicePoint²⁰, which was alleged to have unwittingly sold credit reports to a ring of identity thieves. In the ChoicePoint case, the FTC collected millions of dollars in consumer redress and civil penalties, including a \$10 million civil penalty in connection with the unauthorized disclosure of “nearly 10,000 credit reports,” which were allegedly sold by ChoicePoint to persons without a permissible purpose. At the time, that was the largest fine ever obtained by the FTC.

¹⁸ FCRA § 611

¹⁹ FCRA § 607(b).

²⁰ See Federal Trade Commission, “ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress” (January 26, 2006), (accessed February 22, 2018), <https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million>.

The federal FCRA has been around for nearly 50 years, with occasional fine tuning. Two significant revisions occurred in 1996 & 2003 and in 2012 CFPB began supervision and examination of the credit reporting companies for compliance with the FCRA²¹.

State Law – State Attorney General Enforcement & Breach Notification

In addition to these federal regulatory frameworks, credit reporting companies also have numerous data security obligations under state law. First, credit reporting companies may be subject to data security enforcement of state “mini-FTC Acts” that prohibit unfair or deceptive acts or practices²². Further, at least thirteen states require businesses that own, license or maintain personal information to implement and maintain reasonable security procedures and practices and to protect personal information from unauthorized access, destruction, use, modification or disclosure²³. The majority of states require businesses to dispose of sensitive personal information securely²⁴.

²¹ Importantly for this discussion – the CFPB does not have supervisory authority over data security matters.

²² See, e.g., Becerra, Xavier, California Attorney General, “Attorney General Becerra: Target Settles Record \$18.5 Million Credit Card Data Breach Case” (May 23, 2017), (accessed February 22, 2018), <https://oag.ca.gov/news/press-releases/attorney-general-becerra-target-settles-record-185-million-credit-card-data>.

²³ See National Conference of State Legislatures, “Data Security Laws – Private Sector” (January 16, 2017), (accessed February 22, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

²⁴ See National Conference of State Legislatures, “Data Disposal Laws” (December 1, 2016), (accessed February 22, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>. At the federal level, the FTC’s Disposal Rule regulates the proper disposal of consumer report information. See 16 C.F.R. pt. 682.

Moreover, nearly every state, DC and several U.S. territories have enacted laws requiring notification to affected individuals following a breach of personal information²⁵. These laws typically, but do not always, exempt institutions that are supervised by the federal bank regulators, who have their own breach notice regime. In contrast, credit reporting companies – which are not supervised by the bank regulators – must comply with the patchwork of more than four dozen breach notification laws if a breach does occur.

Contractual Obligations Imposed Due to Other Regulatory Frameworks

Even beyond these direct governmental requirements, the three nationwide credit bureaus – Equifax, Experian and Transunion – are also subject to additional legal requirements resulting from doing business with other major financial institutions. The information security programs at many credit bureau financial institution customers are supervised by federal prudential regulators, i.e., the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation or the National Credit Union Administration. Under comprehensive and detailed information security standards published by the Federal Financial Institutions Council (FFIEC), these financial institutions must oversee the information security programs of their third-party service providers²⁶. Pursuant to these FFIEC requirements, financial institutions and their auditors subject the nationwide credit bureaus to dozens of

²⁵ See National Conference of State Legislatures, “Security Breach Notification Laws” (April 12, 2017), (accessed February 22, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

²⁶ See FFIEC, IT Examination Handbook Infobase, “Information Security: Oversight of Third-Party Service Providers,” (accessed February 22, 2018), <https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers.aspx>.

information security audits each year, many of which include onsite inspections or examinations.

The Payment Card Industry Data Security Standard

The three nationwide credit bureaus also comply with the Payment Card Industry Data Security Standard (“PCI DSS”). The PCI DSS is a set of cybersecurity requirements that are mandatory for all organizations that store, process and transmit sensitive payment card information of the major credit card associations. The standard requires credit reporting companies to take a number of specific steps to ensure the security of certain information. For example, the PCI DSS requires members to install and maintain firewalls, encrypt the transmission of cardholder data, protect against malware and implement and update anti-virus programs, restrict both digital and physical access to cardholder data, regularly test security systems and processes and maintain a detailed information security policy for all personnel. The standard imposes further detailed and specific technical requirements for the protection of cardholder data, such as a restriction on service providers’ storage of personal identification or card verification numbers after card authorization. In addition, the standard requires a service provider to ensure that any third parties with whom it shares data also comply with the PCI DSS²⁷.

²⁷ Payment Card Industry Security Standards Council, “Requirements and Security Assessment Procedures, Version 3.2” (April 2016).

CFPB Supervision

While CRAs had been subject to FTC and state law requirements, in 2012 the CFPB became the first *supervisor* of the national credit reporting system, under authority granted to the Bureau by the Dodd Frank Wall Street Reform and Consumer Protection Act. The Bureau has examination authority over the credit reporting companies, users of credit reports and companies that furnish information into the credit reporting companies for incorporation into credit reports²⁸.

Since CFPB supervision began, the nationwide credit bureaus have been subject to essentially continuous examination cycles, where they have been examined for the adequacy of their compliance management systems, their dispute handling procedures, their procedures to ensure the maximum possible accuracy of credit reports, their credentialing procedures and other important and highly regulated functions. In this supervisory role, the CFPB examines the policies, procedures, controls and practices of credit reporting companies. If the examiners discover any areas in which a credit reporting company is not living up to its obligations, the CFPB can resolve the issue through the supervisory process, or, if the issue is sufficiently serious, choose to bring enforcement actions. The Bureau recently opined on the success of this regime, concluding that it had produced a “proactive approach to compliance

²⁸ The CFPB has supervisory authority over “larger participants” in the consumer reporting industry, which are defined in 12 C.F.R. § 1090.104.

management” that “will reap benefits for consumers – and the lenders that use consumer reports – for many years to come.”²⁹

Legislative Proposals

H.R. _____, the Data Acquisition and Technology Accountability and Security Act

CDIA and our members strongly support a single, preemptive data breach standard for companies across the economy.

Because of the unique liability consumer reporting agencies face under the Fair Credit Reporting Act, such as uncapped statutory damages in class action settings, we believe data breach legislation should be both preemptive of state law and be limited to administrative enforcement. Establishing a uniform national breach standard should not be an opportunity to open up a new cottage industry of trial lawyers suing companies because of technical violations with no consumer harm. Standards should be enforced by the Federal Trade Commission.

A federal data security standard should be flexible and scalable, taking into account the size, scale, scope and sensitivity of the data an organization maintains. The standard should also consider the cost to the enterprise of securing the data. Consumers who are at risk of economic loss as the result of a breach should have timely notice, as should law enforcement and regulators. In addition, consumer reporting agencies should be provided advanced notice

²⁹ See CFPB, “Supervisory Highlights: Consumer Reporting Special Edition, Issue 14, Winter 2017 (March 2017) (accessed February 22, 2018), http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

of a breach so they can be ready to handle the volume of consumer calls that are directed toward them in the case of a breach notification.

The legislation before the Subcommittee today establishes a national standard for both data security and how companies inform impacted people about breaches of the kind of personal information that can be used to set up an account or engage in a financial transaction. The bill's provisions would allow a company's functional regulator to enforce these rules (such as a bank regulator), setting up the FTC as the default regulator for those without a designated regulatory body, with enforcement by state Attorneys General. Since credit bureaus are financial entities under GLBA, they would continue to be subject to the FTC's Safeguards Rule and to civil penalty authority for violations of the breach notification provision of the bill.

The bill's data security provisions for non-financial entities are patterned after those in the Gramm-Leach-Bliley Act, the FTC Safeguards Rule and the Interagency Guidelines referenced earlier. However, the standards in this bill are different -- safeguards would be developed by the covered entities themselves rather than by their regulators. The FTC would not issue regulations implementing this standard for non-financial entities.

The trigger for what constitutes a data breach, "reasonable risk that the breach of data security has resulted in identity theft, fraud, or economic loss," is a fair approximation to how a breach should be defined in any reasonable setting. Companies who have experienced a breach must

“immediately notify without unreasonable delay”; CDIA suggests “without unreasonable delay” (i.e. not including the word “immediately³⁰”), would be more appropriate.

CDIA is pleased to note that for breaches over 5,000 consumers, credit bureaus can be notified ahead of the general notification. This would help ensure that credit bureaus can prepare our systems for increased consumer contacts that a large breach can generate.

This legislation broadly conforms to the policy goals CDIA members have had for breach notification legislation. As the legislative process moves forward, we anticipate that perfecting amendments may further improve the bill³¹, and we look forward to working with the bill sponsor and other members of the Committee on solving this important problem.

H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology (PROTECT) Act of 2017

H.R. 4028 seeks to secure consumers’ credit information by establishing a uniform national standard on how consumers can freeze their credit reports, creates new standards for the regulation of data security at national CRAs and stops the use of Social Security Numbers (SSNs) in credit reporting.

³⁰ Use of the word “immediately” without qualification would suggest that companies would have to disclose the breach before they understand the extent of the breach, have informed law enforcement or closed the vulnerability.

³¹ For example, the bill’s “substitute notice” provisions could be improved to make it more similar to a number of state laws.

Credit freezes were created to assist victims of identity theft. While they may be useful for some victims of identity theft to help protect their credit, they should not be the first line of defense in identity protection. Instead, consumers should check their free annual credit report to review the credit report for any suspicious activity. Consumers may also consider obtaining credit monitoring services, which are routinely provided free of charge to data breach victims.

An initial fraud alert is the first line of defense for consumers who believe that they are, or are about to become, victims of identity theft. This step may be appropriate for consumers who expect to be credit-active. For free, a consumer can place the initial fraud alert by phone, in writing or via website. If a fraud alert is on a consumer's credit file, lenders are required to contact the individual or take reasonable steps to verify the identity of the applicant before extending a new line of credit or increasing a line of credit. A fraud alert requested at one bureau is shared with the other two bureaus. An "extended alert" beyond the initial 90 days will help consumers who are victims of identity theft, but expect to be credit-active.

Members of the military can place an "active duty alert," which lasts for a year and is another preventative option. Fraud alerts were created by CRAs, and were codified as part of the FACT Act of 2003.

Credit freezes are required by law in every State and are a final line of defense for consumers who are chronically victims of identity theft or who do not plan to be credit active or active in various other commercial situations. Different states permit different fees for setting a freeze. A freeze is, effectively, a consumer telling a credit bureau not to release a credit report unless

the consumer contacts the credit bureau in advance to say otherwise. Such a consumer can only obtain credit by taking the extra step of contacting the credit bureau ahead of time. A freeze remains on the file until the consumer lifts or removes the freeze. While a freeze is in place, the consumer's file continues to be updated to reflect current account balances and payments, as well as for account management and collection processes.

The PROTECT Act aims to establish a uniform standard for freezes. Establishing such a system would eliminate consumer confusion on how to place a freeze and reduce administrative costs by having a single standard for compliance. CDIA's impacted members support the freeze language in H.R. 4028.

The PROTECT Act also establishes a new data security supervisory agency for CRAs. As discussed earlier, the consumer reporting industry is currently regulated in many different ways by many agencies. Specifically, the FTC is the industry's primary regulator, and the CFPB supervises certain aspects of our business. We are also regulated indirectly through the federal financial regulators, through their guidance on service providers and vendors.

We continue to believe that the security incident at Equifax should be fully investigated, and stand ready to work with Congress to address regulatory gaps if any are found.

The PROTECT Act would eliminate the use of SSNs by CRAs by 2020. CDIA and its members believe that this is not a feasible proposal and look forward to working with the bill's sponsor

and the Committee on alternatives to this legislation as well as potential innovations in the market.

The SSN has been with us since 1936, and though originally conceived as an identifier for a specific purpose, over time it has become the major individual identifier in the United States. The federal government began this process, expanding the use of the SSN first in 1943 and later in 1961 and beyond. The IRS and DOD have been using the SSN as an identifier of taxpayers and military personnel since the 1960's. In the 1980s, this process accelerated, and the SSN began being used for employment eligibility verification, military draft registration, driver's licenses and for operators of stores that redeemed food stamps. In the 1990s, SSN usage expanded into jury selection, federal workers' compensation laws and through welfare reform legislation³².

The widescale usage of SSNs did not happen overnight; it was a decades long process led by Congress and the Executive Branch.

CRAs need SSNs because we have obligations under the FCRA and other statutes to ensure maximum possible accuracy of the data we maintain. The use of SSNs is absolutely critical to meeting this legal obligation. There simply is no other identifier currently in existence that gives us the ability to match consumers with their information with the confidence required to

³² Hearing on the Homeland Security Threat from Document Fraud, Identity Theft, and Social Security Number Misuse, before the Senate Committee on Finance, Sept. 9, 2003 (statement of James B. Lockhart, III, Deputy Commissioner of Social Security, Social Security Administration).

meet our statutory obligation. If we could not use SSNs, credit reports and other documentation would become less reliable and less useful to lenders when making credit decisions.

SSNs are collected by courts for a number of reasons: identification of parties, collection of fines and restitution, facilitation of the collection of judgments by creditors and governments, etc. Courts notify the Social Security Administration that individuals are incarcerated. Without the use of SSNs, the justice system would grind to a halt. And credit bureaus are part of the process courts use to ensure that child support is paid and that information on a credit file is in line with what a court has ruled. Federal law requires state courts to place SSNs in divorce decrees, child support orders and paternity determinations to facilitate child support collection³³.

The lack of full Social Security Numbers and other identifiers has led to a number of liens and judgements no longer appearing on credit reports. Some courts have limited identifying information in their documents and as a result CRAs can no longer be sure that certain liens or judgements apply to a particular consumer. This creates problems across the economy, as a bank may be asked to loan significant funds to an individual subject to a court judgement, and if the consumer does not disclose it, the institution must use some other way to determine if the

³³ Hearing on Enhancing Social Security Number Privacy: Before the Subcommittee on Social Security of the House Ways and Means Committee, June 15, 2004 (107th Cong.) (statement of Mike L. Buenger, President, Conference of State Court Administrators).

debts listed on an application are comprehensive. Service providers provide that service today, but at additional cost.

The private sector uses SSNs for the same reasons as the government: it is the only reliable and universal identifier. It helps ensure that credit reports are accurate and that information is matched with the correct file. It also helps to ensure that when a business requests a credit report about a consumer, the credit bureau is able to return information regarding the correct individual. Millions of Americans share a name and a surprising number of people share a name and date of birth³⁴. Not everyone has a driver's license. Both the public and private sectors need some way to identify people on documents.

However, there should be limitations placed on how SSNs are used. For example, while SSNs are excellent identifiers and are essential for ensuring data accuracy, they should not be used as a sole method to authenticate an individual's identity. No financial institution or other user of a credit report should be using the SSN as a sole means of authenticating the identity of an individual³⁵. And the bulk of industry follows that guidance – if they did not the incidence of new account fraud would be significantly higher. The fact is that financial institutions have many ways of authenticating an individual, without using the SSN. The technology for use in authenticating individual identity is constantly evolving to stay ahead of perpetrators of fraud.

³⁴ Barr, Joseph R. "The Trouble with Names/Dates of Birth Combinations as Identifiers." ID Analytics, Inc. White Paper (April 2011) (accessed February 22, 2018), https://www.idanalytics.com/media/The_Trouble_With-Names_White_Paper_FINAL.pdf

³⁵ Section 326 of the USA Patriot Act does list the SSN as one of the Personally Identifiable Information data elements that a lender must gather as part of the Know Your Customer rules.

Given the many, many public and private sector uses of the SSN, it would be a monumental undertaking to re-code systems cutting across the entire financial services ecosystem (not just consumer reporting agencies) to some new universal identifier and, further, there would be no means of establishing agreement on what other source should be used or created and how consumers themselves would learn how to use this new identifier in lieu of the SSN. This would not be something that could be done in a matter of 22 months. It would be a years-long system migration costing billions of dollars across the economy.

And even if we determined that we do need to move off of SSNs, the question remains what it would be replaced with. The public and private sectors would still need some kind of universal, unique identifier that can be used across platforms and technologies. In order for it to be universal, it would have to be in federal law. Individual companies have been working to innovate in this field, but how would a private company ensure that every person in the country has an identifier? This is a difficult challenge.

We look forward to working with the bill's sponsor and all of the Members of the Committee to address this challenge. The way to get at this issue is innovation, but unfortunately this challenge has not yet been overcome.

The consumer reporting industry welcomes efforts to establish a national data breach notification, security and credit freeze standards and to make cybersecurity improvements at the national CRAs. While we believe that parts of the PROTECT Act can be improved, we

appreciate the opportunity to address our industry's regulatory structure. Our industry will continue to work with Congress and the regulatory bodies to ensure the security of consumer information.

Especially in the wake of the security incident announced by Equifax in September, CDIA members are doing everything in their power to ensure consumers have confidence their data are in good hands. Data security is not just our regulatory and legal obligation; it is good business. And it is the right thing to do – for consumers, for our customers and for the entire financial system.

Thank you for the opportunity to appear before you. I look forward to your questions.



March 7, 2018

Testimony of
Jason Kratovil

On behalf of

The Financial Services Roundtable

Before the

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

Hearing entitled

“Legislative Proposals to Reform the Current Data Security and Breach Notification
Regulatory Regime”

Chairman Luetkemeyer, Ranking Member Clay and Members of the Subcommittee, thank you for having me here today. On behalf of the leading banking and payments members of the Financial Services Roundtable, I appreciate the opportunity to discuss two very timely and important legislative proposals: A discussion draft of data security and consumer breach notification legislation titled the Data Acquisition and Technology Accountability and Security Act offered by the Chairman and Congresswoman Carolyn Maloney; and H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017, or the PROTECT Act, offered by Congressman Patrick McHenry.

Data is increasingly the engine of modern commerce. For the financial services industry, the proliferation of data has been a catalyst to tremendous innovation. New technologies and analytical tools allow financial institutions of all sizes to assist their customers with financial management and retirement savings, for example, in more sophisticated and more secure ways than ever before.

For other sectors, economies of scale present far less of a barrier to entry today than they did even a decade ago, enabling the smallest firms to purchase the hardware and software – and engage the services of leading global technology and payments firms – to help them process and analyze data, provide better customer service and enhance business efficiencies.

Data held by private companies – and what can be extrapolated from that data – presents tremendous opportunity for consumers across the economy, but also raises new ethical, privacy and security questions as well.

The two proposals up for discussion today touch on the core of many of these questions: What companies have my data? How are those companies protecting it? If they lose my data will I find out, and when? What is the federal government's role in keeping my data secure?

H.R. 4028, the PROTECT Act

This legislation seeks to accomplish three goals: First, require supervision and examination of the cybersecurity practices of the nationwide credit reporting agencies (CRAs); second, create a nationwide standard for consumer security freezes on their credit reports; and third, prohibit the use of consumer Social Security numbers (SSNs) in a credit report or as a means to identify an individual consumer by CRAs effective January 1, 2020.

The nationwide CRAs play a vital role in the provisioning of credit to many American consumers. Their core product -- consumer credit reports -- are multi-year retrospectives on how an individual managed their finances and how much credit he or she has been extended. It provides important insights for any financial institution seeking to evaluate the potential risk presented by an applicant for a variety of financial products, such as credit cards, mortgages, or personal loans. When a consumer wants to access a credit report, CRAs must attempt to *identify* (i.e. "Which 'John Smith' is requesting the file?") and *authenticate* ("Is this 'John Smith' actually who he says he is?") that individual to keep their file separate and distinct from every other individual on which they maintain a file. This requires a sophisticated identity proofing process based on a large body of knowledge specific to each individual consumer.

In other words, CRAs -- understandably -- hold a tremendous amount of information about every credit-active American consumer.

Consumer Reporting Agency Cybersecurity

CRAs are subject to the Federal Trade Commission's (FTC) authority under the Gramm-Leach-Bliley Act (GLBA) with respect to information security. Under the FTC's "Safeguards Rule," CRAs are required to have standards in place to safeguard customer information.¹ Title I of the PROTECT Act makes clear, however, that CRAs currently do not have proactive, ongoing oversight of their data security practices. Two observations:

- Banks, including their significant service providers, are subject to rigorous ongoing oversight and examination of their cybersecurity practices -- in some cases by multiple regulatory bodies -- and hold much of the same data on consumers as the CRAs. Thus:
- Mr. McHenry's proposal accurately identifies a gap -- supervision and examination -- that cannot be filled by the FTC in its capacity as an enforcement-only agency.

National Security Freeze

Every state and the District of Columbia have enacted legislation allowing consumers to place a freeze on their credit file.² In that respect, a national standard such as the one proposed in the PROTECT Act would smooth out the inconsistencies that currently exist

¹ See 16 CFR Part 314, accessed at: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>

² <http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx>

across state laws. For consumers, it is reasonably certain that with a freeze in place a fraudster could not access a consumer's credit to commit identity theft.

However, there are also potential consumer disadvantages from having a credit freeze in place. For instance, it is also reasonably certain that with a freeze in place, it is not possible for the consumer to obtain credit at all. This can be very disruptive. For example, consumers very often encounter pressing needs or emergencies that may necessitate quick access to a new line of credit, which could be blocked if a consumer has not taken the appropriate steps or allowed sufficient time for the freeze to be lifted. Emergencies – car repairs or a broken water heater – or even routine transactions – buying a new mobile phone, financing the new bedroom set that finally went on sale – become impossible if the consumer forgot to “unfreeze” their file beforehand. Other tools exist – such as fraud alerts, credit monitoring, and the federally mandated availability of a free annual credit report – that may be more appropriate for many consumers.

Credit Rating Agency Use of Social Security Numbers

There is broad consensus among FSR members and beyond that the reliance on SSNs throughout the economy represents a broken system in need of reform. Fundamentally, SSNs were devised as a way to assist the federal government in dispensing benefits to the correct person. That they are now relied upon to both identify and, in many instances, authenticate a person (ostensibly because they are still a “secret”) is a serious problem and increases their value to identity thieves. From a practical perspective, data breaches have exposed the SSNs of so many consumers that the case can be credibly made that everyone should stop pretending SSNs are any more confidential than information readily accessed in a phone book or five-second Internet search.³ Recognizing this reality would make the continued use of SSNs as *identifiers* by CRAs and others far less problematic. The key is finding alternatives to the use of SSNs as *authenticators* of an individual, which requires much more effort.

To that end, the proposal to prohibit the use by CRAs of SSNs is certainly positive in driving a conversation on the future of digital identities. In fact, FSR members are actively engaged in charting a path toward a future built around trusted frameworks and standards for proving the identity of a person without a reliance on SSNs or passwords. Technological improvements will make this easier and firms are increasingly

³ For more, see testimony of Jeremy Grant, Managing Director, Technology Business Strategy, Venable LLP before the U.S. House Committee on Energy & Commerce Subcommittee on Oversight and Investigations, hearing titled “Identity Verification in a Post-Breach World,” 11/30/2017. Accessed at: <http://docs.house.gov/meetings/IF/IF02/20171130/106662/HHRG-115-IF02-Wstate-GrantJ-20171130.pdf>

experimenting with new methods that leverage behavioral data, biometrics, tokenization, geolocation and telematics, but this will take time to mature across the ecosystem.

Given the current state, I would make the following points to support our belief that the outright prohibition on SSN use as contemplated in the PROTECT Act is not advisable as a matter of legislative policy:

- First, viable alternative systems to replace SSNs are many years from becoming reality and will require not only significant work on the part of the private sector, but also the support and engagement of federal and state governments. Eventually, industry and government will develop new trusted methods to authenticate an individual that don't require SSNs, making their continued use as an identifier fairly harmless. Resources should be focused into these efforts, not into the scramble to find a new method of identifying a consumer that would inevitably be triggered were this measure to become law.
- Second, in many instances, the use of SSNs by financial institutions is required by federal rules and regulations. Unravelling SSNs from the fabric of financial services, as this measure would potentially require, will necessitate significant revisions to many federal rules and regulations that today obligate financial institutions to utilize SSNs to meet a variety of regulatory requirements.⁴ That process will take time.
- Third, banning the use of SSNs as identifiers by the CRAs would make it very difficult for financial institutions to detect and stop instances of synthetic identity fraud.⁵ This type of identity theft, which disproportionately affects the SSNs of children and is estimated to cost financial institutions \$6 billion in losses each year,⁶ can be dramatically reduced when institutions are able to verify whether or not a given name, date-of-birth and SSN correspond to what the SSA has on file. In fact, discussions are underway with Members of this Committee, your colleagues

⁴ See Appendix A.

⁵ Synthetic identity fraud involves the creation of a fake identity and credit file, often by using a combination of real data (most often SSNs of children) from multiple individuals and fabricated information. To carry out financial fraud, the fictitious identity and associated credit file is leveraged over time to build a positive history that allows the fraudster to ultimately apply for and obtain new credit. This new credit is quickly maxed out and, of course, never repaid. This immediate loss is absorbed by the financial institution. However, the child whose SSN was compromised may have no awareness that their information was used to commit synthetic identity theft until the first time he or she applies for credit, a student loan, etc., many years after the fraud has been committed. For more, please see: "Why Children are now Prime Targets for Identity Theft," accessed at: <http://thehill.com/opinion/cybersecurity/373692-why-children-are-now-prime-targets-for-identity-theft>.

⁶ "Synthetic Identity Fraud Cost Banks \$6 Billion in 2016: Auriemma Consulting Group," *Markets Insider*, August 1, 2017. Accessed at: <http://markets.businessinsider.com/news/stocks/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group-100222563>

on the Ways & Means Committee and in the Senate to modernize and enhance the ability of SSA to assist in fighting synthetic identity fraud. Senators Tim Scott (R-SC), Claire McCaskill (D-MO), Bill Cassidy (R-LA) and Gary Peters (D-MI) recently introduced the Protecting Children From Identity Theft Act, S. 2498, legislation that would help prevent synthetic identity fraud by improving the ability of financial institutions and CRAs to validate SSNs as consumer identifiers to flag and stop their misuse.

- Finally, CRAs are merely one segment of one sector of the economy. I would encourage policymakers to address this issue from a more holistic perspective: The overuse and over-reliance of SSNs is not limited to the CRAs, and prohibiting their use by this single slice of the economy is far from a cure to the overall problem. As mentioned, Congress has an essential role to play in facilitating public-private collaboration toward a set of solutions that works for every consumer and business in the United States that has a need to accurately verify their own identity, or the identity of a prospective customer. A piece-by-piece approach is likely to create more confusion and problems than it is likely to solve.

Discussion Draft: The Data Acquisition and Technology Accountability and Security Act

I have been engaged in this Committee's efforts on data security and consumer breach notification legislation in various capacities since the introduction of H.R. 3997, the Financial Data Protection Act of 2005, by my then-employer the late Rep. Steven C. LaTourette (R-OH), along with Reps. Darlene Hooley (D-OR), Mike Castle (R-DE), Deborah Pryce (R-OH) and Dennis Moore (D-KS). This first comprehensive, bipartisan bill passed this Committee but then, as has been the fate of every subsequent piece of data security legislation, could not be reconciled with competing legislation from the Energy & Commerce Committee and thus never reached the House floor.

For 13 years, I and many others who have worked to advance federal data security legislation have watched as countless high-profile breaches came and went, each presenting an opportunity for Congress to respond, only to see bills fail to get beyond a single committee's process. Even in the last Congress, when legislation sponsored by Reps. Randy Neugebauer (R-TX) and John Carney (D-DE)⁷ passed this Committee by an overwhelming vote of 46-9, that was not enough momentum to advance to the House floor.

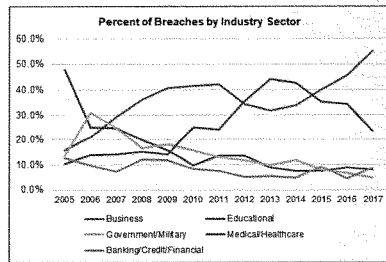
⁷ H.R. 2205, the Data Security Act of 2015.

Which begs the question, what will it take? To be sure, the devil most definitely is in the details when crafting strong federal legislation that strikes the right balance between protecting consumers with strong data protection requirements while providing timely, risk-based notification of a breach. Historically, this has led to divisions between industries that, unsurprisingly, followed jurisdictional lines between the relevant committees. While some of those divisions still remain, there is increasingly a desire among many industries to work together to support Congressional efforts to get a bill done. This was highlighted recently when 23 trade groups – representing financial services, technology, telecommunications and retail – signed a letter⁸ to your colleagues on the House Energy & Commerce Committee outlining shared policy priorities. This was actually the first time such a broad group of industries has come together in any capacity on this issue. It is FSR's hope that finding consensus among these diverse stakeholders will help advance the efforts of this Committee and other committees of jurisdiction to advance legislation through the full House.

Overview

The entire financial services industry – from the leading members of FSR to the thousands of community banks and credit unions in this country – are united in our goal to protect consumers and prevent data breaches. Trust and confidence are hallmarks of our industry: Consumers have come to expect their financial institution will be a good steward of their money. While no industry is perfect, it's for good reason that financial firms are held up as leading the economy in security and security-related innovation.

As the data shows, no business or industry segment is immune to hackers. Financial institutions are, not surprisingly, frequent targets of hackers. As Robert Novy, Deputy Assistant Director at the U.S. Secret Service put it: "US financial and payment systems were, and remain, the



Source: ITRC Data Breach Report 2017

natural target for much of this criminal activity – for the simple reason, as the bank robber Willie Sutton was once reported to have quipped, 'That's where the money is at.'⁹

⁸ See Appendix B

⁹ See 2017 Verizon Data Breach Investigations Report, Appendix B.

As the data also makes clear, despite the prevalence and frequency of attacks, the financial industry continues to make the necessary investments that have minimized the overall frequency of data breaches within our industry. Cybersecurity is a regular discussion item from the first line operating level all the way up to Executive Management teams and the Board of Directors. For many FSR members, for example, cybersecurity is a discussion item for the full Board and Board Committees on a quarterly basis, if not more often.¹⁰

More innovation is taking place throughout the payments ecosystem than in arguably any other aspect of financial services. From increasing security and reducing fraud to creating a more friction-free experience for consumers, our industry is committed to building and implementing the systems to maintain our role as consumers' trusted source for payments and managing money. New methods of biometric authentication, cloud-based technology, location-based services, and keystroke behavior patterns will be the norm in the future.

More immediately, tokenization – which replaces sensitive financial information with data that can only be interpreted by a very limited set of parties in the transaction chain, but is of no value if stolen in a data breach – is paving the way for mobile payments to become a widely adopted method of payment consumers can trust. Tokenization, along with biometrics to help in customer authentication, are the key security drivers that brought Apple Pay and other digital wallets to market creating what is, according to many, the most secure payment experience available.¹¹

The security technology behind Apple Pay is a good example of how a layered approach – incorporating a variety of technologies – is needed to ensure consumer data is protected. Again, there is no single panacea to preventing fraud and stopping data breaches.

This Discussion Draft, however, is a very positive step forward to filling an important policy void.

¹⁰ See FSR/BITS "Deciphering Cyber for Your Board of Directors." Available at <http://www.fsroundtable.org/wp-content/uploads/2017/10/FSR-BITS-Deciphering-Cyber-for-Your-Board-of-Directors-Facilitating-a-Better-Dialogue.pdf>

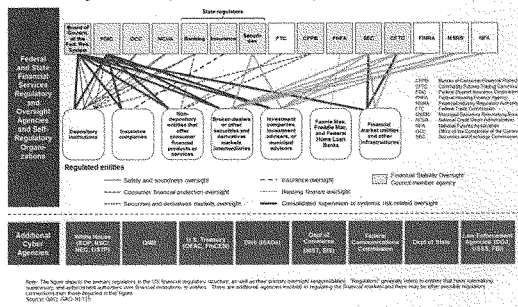
¹¹ <http://mashable.com/2014/10/23/apple-pay-is-more-secure-than-your-credit-and-debit-cards/>

Protection of Information

Overview

According to a report published by Homeland Security Research Corp., the financial services cybersecurity market in the United States reached an estimated \$9.5 billion in 2016, making it the largest non-government cybersecurity market.¹² Of that number, the top four U.S. banks spent nearly \$1.5 billion.¹³ In addition, other reports indicate that firms within the financial sector "...spend more on IT security than any other sector, spending three times as much as comparably sized non-financial institutions."¹⁴

As members of this Subcommittee are well aware, cyber and data protection practices of the financial industry are overseen by nine independent federal regulators, three self-regulatory organizations, the U.S. Department of the Treasury as it sector-specific agency, and every state banking and securities agency. When agencies tasked with cyber-related authorities are added, the list expands even further.



While FSR and its members are actively working to harmonize many of these complexities, our members appreciate the need for robust oversight and regulation of our cybersecurity practices.

All of these obligations stem from a single law, the Gramm-Leach-Bliley Act (Pub.L. 106-102) (GLBA), enacted in 1999. Section 501(b) of Title V of this law directed federal and state regulators with oversight of financial institutions and the FTC to establish

¹² See: <http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/>
¹³ See: <https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-bofa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#7204cf13116d>
¹⁴ See: https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf.

appropriate standards and processes relating to administrative, technical and physical safeguards to protect customer information.

We are not suggesting that all unregulated sectors of the economy be subjected to comparable levels of regulatory burden and oversight, nor would this make sense or even be feasible: Most firms across the economy have minimal or no exposure to consumers' sensitive financial or personal information that would warrant this level of intense cybersecurity oversight. It should also be noted that no government examination agency even exists with the capacity to conduct such oversight of every business in the country.

However, FSR strongly believes Congress needs to act to require firms of all shapes and sizes that handle sensitive information to protect the data, and it should do so by creating a robust, yet flexible and scalable, data security framework.

On the Discussion Draft

The approach detailed in the Discussion Draft strikes the appropriate balance by setting a high bar for data protection, while providing numerous considerations to ensure a small business that processes or maintains little or no personal information is not burdened with the same expectations as a larger entity.

The standards and processes produced as a result of Title V of GLBA provide a useful comparison: GLBA's implementing regulations include a similar set of considerations as the Discussion Draft outlines in section 2(a)(2). These GLBA standards apply to the smallest credit union or community bank and the largest member of FSR. There are no carve-outs for institutions under a certain asset size: Instead – and the rules the financial industry follows on this are explicit – the tools our industry employs to protect customers must be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the information it handles. These considerations have demonstrated that the most robust cybersecurity expectations can be appropriately tailored to firms that differ dramatically in their data protection needs.

Furthermore, the Discussion Draft refrains from mandating specific technologies. This is a critical point, and speaks to the benefit of legislating a process- and risk-based framework: Picking technological winners and losers in statute is a sure-fire way to suppress innovation and tie the hands of cybersecurity professional seeking to defend their companies against attack. Rigid legal requirements fail to keep up with the dynamic cyber threat environment, forcing companies to focus on compliance rather than building the most effective cyber defenses against criminals.

*Notification of Breach of Data Security*Overview

Similar to the existing requirements for financial institutions to protect customer data outlined above, GLBA also requires financial institutions to maintain customer notification programs that would ensure financial firms provide notice to impacted customers when the financial institution itself suffered a breach.

Some non-financial trade groups continue to make the assertion that banks are not required under GLBA to provide notice to consumers of their own data breach. They base this claim on the fact that the bank regulators issued interagency “guidance” on consumer breach notification which, in their estimation, does not amount to a mandate. This is a false assertion, however, as it fails to recognize that guidance is often treated by prudential regulators in the ongoing oversight and examination process as a requirement that is due the same adherence as law or regulation.

As such, before discussing the notice provision of the Discussion Draft, I would like to take this opportunity to explain how financial institutions are, in fact, required to maintain breach incident response programs:

- In 2005, the federal banking agencies jointly issued interagency guidance (interpreting Section 501(b) of GLBA and the Interagency Guidelines) concerning how a financial institution must respond to the unauthorized acquisition or use of customer information.¹⁵
- This Guidance is a Safety and Soundness standard issued under the federal banking agencies’ safety and soundness authority under Section 39 of the Federal Deposit Insurance Act,¹⁶ as well as under Section 501(b) of GLBA.¹⁷
- Federal banking agencies examine financial institutions for their compliance with the Guidance. In this regard, the Guidance is not treated as a recommendation: It is a Safety and Soundness standard for which compliance is demanded.
- The federal banking agencies may fine or otherwise penalize a financial institution for its failure to comply with the Guidance, by – as an example – issuing Matters Requiring Attention (MRAs). As an illustration, in reference to the notification

¹⁵ 12 C.F.R. pt. 364, App. B (FDIC); 12 C.F.R. pt. 208, App. D-2 and pt 225, App. F (FRB); 12 C.F.R. pt. 30, App. B (OCC). See also 70 Fed. Reg. 15,736 (Mar. 29, 2005).

¹⁶ See <https://www.fdic.gov/regulations/laws/rules/1000-4100.html>

¹⁷ See, E.G., 12 C.F.R. 30.2.

Guidance, the Office of the Comptroller of the Currency (OCC) states: *The OCC may treat a bank's failure to implement the final guidance as a violation of the Security Guidelines that are enforceable under the procedures set forth in 12 USC 1831p-1, or as an unsafe and unsound practice under 12 USC 1818.*¹⁸

- If the financial institution determines misuse of the information "has occurred or is reasonably possible," the financial institution "should notify the affected customer as soon as possible." The Guidance uses the term "should" to express a financial institution's obligation or duty to notify, as opposed to a recommendation. That is, the Guidance *requires* notice in accordance with its standards, as opposed to only recommending notice.
- The Guidance states that financial institutions have "an affirmative duty" to protect customer information from unauthorized access or use.¹⁹ In this regard, the Guidance clarifies that "[n]otifying customers of a security incident involving the unauthorized access or use of the customer's information in accordance with the standard set forth [in the Guidance] is a key part of that duty." Again: Notice to customers in accordance with the Guidance is an "affirmative duty."
- The Guidance clarifies that "[w]hen customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so."²⁰
- Notice obligations extend equally with respect to incidents involving customer information at a financial institution's service provider. Specifically, the Guidance provides that where unauthorized access to customer information occurs at a financial institution's service provider, "it is the responsibility of the financial institution to notify the institution's customers and regulator."²¹ Banking agencies further require financial institutions to ensure their service provider contracts address procedures for notifying the institution of security breaches that pose risk to consumers. *Once more: Notice is a responsibility and a duty, not a recommendation.*

Not only do FSR members take the protection of data very seriously, they also prioritize customer service and communication – of both good news and bad. Suggesting these requirements of GLBA are in some way optional is misinformed and misguided.

¹⁸ <http://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-13.html>

¹⁹ See, e.g., 12 C.F.R. pt. 30, App. B, Supp. A, III.

²⁰ See, e.g., 12 C.F.R. pt. 30, App. B, Supp. A, III.

²¹ See, e.g., 12 C.F.R. pt. 30, App. B, Supp. A, II(A)(2).

On the Discussion Draft

- FSR strongly supports a risk-based trigger, which will help ensure consumers are notified when they are actually at risk from a breach. Over-notification leads to desensitization, which can cause consumers to ignore warnings and the need to act that a legitimate risk-inducing data breach notice can provide. The Discussion Draft calls for consumers to be notified when a breach is reasonably likely to result in "identity theft, fraud, or economic loss." While "economic loss" is an extremely broad term that should be clarified, overall this risk-based approach is the appropriate construction.
- On the issue of the timing of notifications, as discussed in the Subcommittee's hearing on February 14, 2018, the key question for policymakers is when legislation should specify the proverbial "clock starts ticking." The Discussion Draft contemplates that the clock starts ticking after the covered entity completes its preliminary investigation required under Sec. 4(a). This is the correct approach: Premature notification – i.e., notice being provided *before* a covered entity has ascertained a fuller picture of the breach, determined whether or not the breach compromised personal information, the loss of which could result in identity theft, fraud or economic loss, and taken initial steps to secure their compromised systems – may result in false alarms. The Discussion Draft sets a practical and balanced standard that will contribute to accurate notification to impacted consumers.
- The Discussion Draft states consumers are to be notified "immediately...without unreasonable delay." The introduction of an "immediate" timeframe for notification is, perhaps, without precedent. Most state laws have adopted a variation on one of two themes: Either "in the most expedient time possible and without unreasonable delay" or simply "without unreasonable delay."²² The Committee should consider any of these similar concepts that can ensure consumers are notified as soon as possible while not creating unnecessary or unwarranted alarm.

Enforcement and Preemption

- The Discussion Draft provides for enforcement over financial institutions by the federal banking regulators, and the Federal Trade Commission (FTC) and state Attorneys General for other sectors that do not have functional oversight. We believe this is an appropriate approach that does not duplicate the ongoing,

²² See Appendix C.

regular enforcement activities of federal bank examiners. *This is an important distinction: Financial institutions have examiners, empowered with significant enforcement tools, overseeing their information security and breach notice responsibilities in an ongoing capacity. Examiners have similar oversight authority over technology service providers to those financial institutions. No other sector subject to this legislation has equivalent oversight and enforcement.*

- Few issues are as ripe for federal legislative action as data security. FSR and others have over the years described the patchwork of conflicting state laws, which illustrates the need for Congress to act in a way that sets one strong, uniform national standard. To echo an important sentiment: Whether or not a person's data is protected should not depend on where they live. That is why FSR firmly believes Congress must enact a robust yet flexible framework for the protection of sensitive information, a threshold achieved by the Discussion Draft.

Conclusion

Data breach and payment security issues are fundamentally about protecting consumers. Every American business that handles sensitive financial information should have an innate motivation to protect it, if for no other reason than maintaining the trust and continued business of their customers.

I would like to conclude by revisiting the key questions I posed at the outset:

What companies have my data? The answer is, more than any of us probably realize. Which is all the more reason for Congress to act to ensure that no matter where the data resides, it is protected.

How are those companies protecting it? Today, they are only required to protect it if the small number of state security laws are applicable to their business. Again, where a person lives should not dictate whether or not their data is required to be protected. That said, setting the appropriately high standard and framework for protection is critical, as is not making specific technology mandates. The Discussion Draft strikes the right balance.

If they lose my data will I find out, and when? Customers must be made aware of a breach when they are at risk, and that notification must happen quickly. That said, the company that suffered the breach needs a reasonable amount of time to ascertain what happened, identify impacted customers, involve law enforcement and secure their systems. This should not be an excuse to drag out notification, however.

What is the federal government's role in keeping my data secure? The sectoral approach adopted by the U.S. has addressed data protection for two of the most sensitive industries: Financial services and healthcare. For the financial sector, that has evolved into comprehensive rules and regulations, enforced by numerous agencies through robust on-site examinations. However, the proliferation and importance of data to every sector of the economy has highlighted the need for the federal government to take steps to keep it secure. Both bills that are the topics of today's hearing take important steps to address these challenges.

Thank you for inviting me to testify. I look forward to your questions.

Appendix A

Federal Laws & Regulations Related to Financial Institutions' Obtaining Social Security Numbers

Statute & Regulation	Social Security Number Requirement	Retention/Disposal Provisions
A. BSA/AML		
Customer Identification Program 31 C.F.R. § 1020.220	Prior to opening an account , the bank/thrift/credit union must, at a minimum, obtain the customer's name, date of birth, address (residential or business), and an identification number (can be taxpayer identification number).	The bank must retain identifying information for five years after the account is closed .
Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks 31 C.F.R. § 1010.415	No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for \$3,000 or more in currency unless it maintains records of the following information , which must be obtained for each issuance or sale of one or more of these instruments to any individual purchaser which involves currency in amounts of \$3,000-\$10,000 inclusive: If the purchaser does not have a deposit account with the financial institution: (A) The name and address of the purchaser; (B) The social security number of the purchaser, or if the purchaser is an alien and does not have a social security number, the alien identification number; (C) The date of birth of the purchaser; (D) The date of purchase; (E) The type(s) of instrument(s) purchased; (F) The serial number(s) of the instrument(s) purchased; and (G) The amount in dollars of each of the instrument(s) purchased.	Records required to be kept shall be retained by the financial institution for a period of five years and shall be made available to the Secretary upon request at any time
Beneficial Ownership 31 C.F.R. § 1010.230 (effective May 11, 2018)	Financial institutions are required to obtain, verify, and record the identities of the beneficial owners of legal entity customers. As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and social security number or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.	A financial institution must retain the records for five years after the date the account is closed.
B. Consumer Financial Products and Services		
Application for a residential mortgage loan (Truth in Lending Act)	For residential mortgage transactions, an application consists of the submission of the consumer's name, the consumer's income, the consumer's social security number to obtain a credit report, the property address, an estimate of the value of the property, and the mortgage loan amount sought.	A creditor shall retain evidence of compliance for two years after the date disclosures are required to be made or

<p>12 C.F.R. §§ 1026.3(a)(3)(ii); 1026.25 Electronic Fund Transfer Act – Error Notice 12 C.F.R. §§ 1005.11 and 1005.13</p>	<p>A financial institution shall comply with the requirements of this section with respect to any oral or written notice of error from the consumer that: (i) Is received by the institution no later than 60 days after the institution sends the periodic statement or provides the passbook documentation, on which the alleged error is first reflected; (ii) Enables the institution to identify the consumer's name and account number; and (iii) Indicates why the consumer believes an error exists and includes to the extent possible the type, date, and amount of the error, except for requests described in paragraph (a)(1)(vii) of this section.</p> <p>Content of error notice. The notice of error is effective even if it does not contain the consumer's account number, so long as the financial institution is able to identify the account in question. For example, the consumer could provide a Social Security number or other unique means of identification.</p>	<p>action is required to be taken.</p> <p>Any person subject to the Act and this part shall retain evidence of compliance with the requirements imposed by the Act and this part for a period of not less than two years from the date disclosures are required to be made or action is required to be taken.</p>
<p>C. Privacy/Information Security</p>		
<p>Privacy of Financial Information 12 C.F.R. pt. 332</p>	<p>Nonpublic personally identifiable information includes any information a consumer provides to you to obtain a financial product or service from you.</p> <p>The regulation:</p> <ul style="list-style-type: none"> (1) Requires a financial institution to provide notice to customers about its privacy policies and practices; (2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and (3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions. 	<p>No specific recordkeeping requirement.</p>
<p>Interagency Guidelines Establishing Information Security Standards 12 C.F.R. pt. 364, App. B (and corresponding regs)</p>	<p>An institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to sensitive customer information, which includes SSN, because this type of information is most likely to be misused, as in the commission of identity theft.</p> <p>Notice to Regulator: The institution's response program must include procedures for notifying its primary federal regulatory as soon as possible when the institution becomes aware of an incident involving unauthorized access to or uses of sensitive customer information.</p>	<p>An institution's information security program must ensure the proper disposal of customer information and consumer information.</p>

	<p>Notice to Consumer: When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.</p>	
D. Identity Theft/Consumer Reports		
<p>Red Flags Rule 12 C.F.R. pt. 334, App. J (and corresponding regs)</p>	<p>Requires financial institutions and creditors to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.</p> <p>Each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts: Suspicious personal identifying information includes:</p> <ul style="list-style-type: none"> • Social security number has not been issued or is listed on the Social Security Administration's Death Master File • Lack of correlation between the SSN range and date of birth • The SSN provided is the same as that submitted by other persons opening an account or other customers. 	
<p>Duties of Consumer Reporting Agencies Regarding Identity Theft 12 C.F.R. § 1022.123</p>	<p>Consumer reporting agencies shall develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity where the consumer asserts a good-faith belief that have been a victim of identity fraud or a related crime.</p> <p>Examples of information that might constitute reasonable information requirements for proof of identity are provided for illustrative purposes only:</p> <p><i>Consumer file match.</i> The identification information of the consumer including his or her full name (first, middle initial, last, suffix), any other or previously used names, current and/or recent full address (street number and name, apt. no., city, state, and zip code), full nine digits of Social Security number, and/or date of birth.</p>	
<p>Disclosure by CRA of Consumer File to</p>	<p>Every consumer reporting agency shall, upon request, clearly and accurately disclose to the consumer all information in the consumer's file at the time of the request, except that if the</p>	

<p>Consumer; Free Annual Report; <i>15 U.S.C. §§ 1681g, 1681h, 1681j(a); 12 C.F.R. pt. 1022, subpart N.</i></p>	<p>consumer to whom the file relates requests that the first five digits of the SSN not be included, and the reporting agency has adequate proof of the identity of the requester, the reporting agency shall so truncate the disclosure.</p> <p>A CRA shall require, as a condition of making that disclosure, that the consumer furnish proper identification.</p> <p><u>Free Annual Reports:</u> There is a centralized source for requesting annual file disclosures from nationwide CRAs which collects only as much personally identifiable information as is reasonably necessary to properly identify the consumer and to process the transaction requested by the consumer.</p> <p>Any personally identifiable information collected from consumers as a result of a request for annual file disclosure, or other disclosure required by the FCRA, made through the centralized source, may be used or disclosed by the centralized source or a nationwide consumer reporting agency only:</p> <ol style="list-style-type: none"> (1) To provide the annual file disclosure or other disclosure required under the FCRA requested by the consumer; (2) To process a transaction requested by the consumer at the same time as a request for annual file disclosure or other disclosure; (3) To comply with applicable legal requirements, including those imposed by the FCRA and this part; and (4) To update personally identifiable information already maintained by the nationwide consumer reporting agency for the purpose of providing consumer reports, provided that the nationwide consumer reporting agency uses and discloses the updated personally identifiable information subject to the same restrictions that would apply, under any applicable provision of law or regulation, to the information updated or replaced. 	
---	--	--

Appendix B

January 4, 2018

The Honorable Greg Walden
Chairman
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Bob Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden and Chairman Latta:

The undersigned organizations, representing companies across the American economy, take the stewardship and protection of customers' personal information very seriously. That is why we support federal legislation to protect personal information and, in the event of a data breach that could result in identity theft or other financial harm, ensure consumers are notified in a timely manner.

We believe that Congress should enact legislation encompassing the following elements:

- A flexible, scalable standard for data protection that factors in (1) the size and complexity of an organization, (2) the cost of available tools to secure data, and (3) the sensitivity of the personal information an organization holds, as well as guarantees that small organizations are not burdened by excessive requirements.
- A notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators when there is a reasonable risk that a breach of unencrypted personal information exposes consumers to identity theft or other financial harm.
- Consistent, exclusive enforcement of the new national standard by the Federal Trade Commission (FTC) and state Attorneys General, other than for entities subject to state insurance regulation or who comply with the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act of 1996/HITECH Act. For entities under its jurisdiction, the FTC should have the authority to impose penalties for violations of the new law.
- Clear preemption of the existing patchwork of often conflicting and contradictory state laws.

Data security impacts every sector of the economy. We therefore look forward to working with you and your colleagues to ensure that all sectors employ sound data security and alert consumers when a breach may result in identity theft or other financial harm.

Sincerely,

ACT | The App Association
American Bankers Association
American Council of Life Insurers
American Insurance Association
American Land Title Association
BSA | The Software Alliance
Consumer Bankers Association
Credit Union National Association
CTIA
Electronic Transactions Association
Financial Services Roundtable
Independent Community Bankers of America
Independent Insurance Agents and Brokers of America
Internet Commerce Coalition
National Association of Federally-Insured Credit Unions
National Association of Mutual Insurance Companies
National Business Coalition on E-Commerce & Privacy
Property Casualty Insurers Association of America
Reinsurance Association of America
Retail Industry Leaders Association
TechNet
Twenty-First Century Privacy Coalition
USTelecom

Appendix C

State Data Breach Notification Laws: Timing of Consumer Notice

STATE	TIMING
ALASKA	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
ARIZONA	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach, to identify residents affected, and to restore the reasonable integrity of the system.
ARKANSAS	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
CALIFORNIA	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
COLORADO	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
CONNECTICUT	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach, to identify those affected, or to restore the reasonable integrity of the system.
DELAWARE	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
DISTRICT OF COLUMBIA	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
FLORIDA	Must be made as expeditiously as practicable and without unreasonable delay but no later than 30 days after the determination of breach, consistent with time necessary to determine the scope of the breach, identify those affected, and restore the reasonable integrity of the system.
GEORGIA	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
GUAM	Must be made without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.
HAWAII	Must be made without any unreasonable delay consistent with any measures to determine contact info, the scope of the breach, and to restore the reasonable integrity, security, and confidentiality of the system.
IDAHO	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the resident affected, and restore the reasonable integrity of the system.

ILLINOIS	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
INDIANA	Must be made without unreasonable delay, consistent with necessary measures to restore the integrity of the system or necessary to discover the scope of the breach.
IOWA	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, sufficiently determine contact info for the residents affect, and restore the reasonable integrity of the system.
KANSAS	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
KENTUCKY	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
LOUISIANA	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the system.
MAINE	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the system.
MARYLAND	Must be made as soon as reasonably practicable after the investigation but after given notice to the Attorney General, consistent with measures to determine scope of the breach, identify individuals affected or restore the integrity of the systems.
MASSACHUSETTS	Must be made as soon as practicable and without unreasonable delay.
MICHIGAN	Must be made without unreasonable delay, consistent any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
MINNESOTA	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify those affected, and restore the reasonable integrity of the system.
MISSISSIPPI	Must be made without unreasonable delay, subject to the completion of an investigation to determine the nature and scope of the breach or to restore the reasonable integrity of the system.
MISSOURI	Must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
MONTANA	Must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
NEBRASKA	Must be made as soon as possible and without unreasonable delay, consistent with any measures necessary to determine the scope and restore the reasonable integrity of the system.

NEVADA	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures to determine the scope of the breach and restore the reasonable integrity of the system.
NEW HAMPSHIRE	Must be made as soon as possible.
NEW JERSEY	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
NEW MEXICO	Must be made in the most expedient time possible, but no later than 45 calendar days following discovery of the breach, subject to the delay provision discussed below.
NEW YORK	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
NORTH CAROLINA	Must be made without unreasonable delay taking any necessary measures to determine sufficient contact info, determine the scope of the breach and to restore the reasonable integrity, security, and confidentiality of the system.
NORTH DAKOTA	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
OHIO	Must be made in the most expedient time possible but not later than 45 days following its discovery of the breach consistent with any measures necessary to determine the scope of the breach, include which consumers' info was accessed or acquired, and to restore the reasonable integrity of the system.
OKLAHOMA	Must be made in the most expedient time possible without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
OREGON	Must be made in the most expeditious time possible and without unreasonable delay and consistent with any measures necessary to determine sufficient contact info, determine the scope of the breach, or restore the reasonable integrity, security, and confidentiality of the data.
PENNSYLVANIA	Must be made without unreasonable delay taking any necessary measures to determine the scope of the breach and to reasonable restore the integrity of the system.
PUERTO RICO	As expeditiously as possible consistent with any measures to restore the security of the system.
RHODE ISLAND	Must be made in the most expedient time possible but no later than 45 days after confirmation of the breach and the ability to ascertain information that must be included in the consumer notice.
SOUTH CAROLINA	Must be made in the most expedient time possible without any unreasonably delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
TENNESSEE	Must be made immediately but no later than 45 days from discovery of the breach.
TEXAS	Must be made as quickly as possible, except as necessary to determine the scope of the breach and restore the reasonable integrity of the system.
UTAH	Must be made in the most expedient time possible without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.

VERMONT	Must be made in the most expedient time possible and without unreasonable delay but not later than 45 days after discovery and consistent with any measures to determine the scope of the breach and to restore the reasonable integrity, security, and confidentiality of the system.
VIRGIN ISLANDS	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
VIRGINIA	Must be made without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
WASHINGTON	Must be made in the most expedient time possible without unreasonable delay but no more than 45 calendar days after the breach was discovered, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
WEST VIRGINIA	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
WISCONSIN	Must be made within a reasonable time not to exceed 45 days, subject to law enforcement delay.
WYOMING	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.



**Written Testimony of
John Miller**

**Vice President, Global Policy and Law
Information Technology Industry Council (ITI)**

**Before the
Subcommittee on Financial Institutions and Consumer Credit
U.S. House Committee on Financial Services**

**“Legislative Proposals to Reform the Current Data Security
and Breach Notification Regulatory Regime”**

March 7, 2018



Written Testimony of:
John Miller
Vice President, Global Policy and Law

Information Technology Industry Council (ITI)

Before the:
Subcommittee on Financial Institutions and Consumer Credit
U.S. House Committee on Financial Services

**"Legislative Proposals to Reform the Current Data Security and Breach Notification
Regulatory Regime"**

March 7, 2018

Chairman Luetkemeyer, Ranking Member Clay, and Members of the Subcommittee, thank you for the opportunity to testify today on the *Discussion Draft of H.R. ____, the Data Acquisition and Technology Accountability and Security Act* (hereinafter, the "discussion draft"). My name is John Miller, and I am the Vice President for Global Policy and Law at the Information Technology Industry Council (ITI). ITI, the global voice of the tech sector, represents over 60¹ of the world's leading information and communications technology (ICT) companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, internet companies, and companies using technology to fundamentally evolve their businesses. Privacy and cybersecurity policy are rightly a priority for governments and our industry, and we share common goals of protecting the privacy of individuals' data, improving cybersecurity, and maintaining strong consumer protections.

Cybersecurity and network and data protection technologies are critical to ITI members. Facilitating the protection of our customers, including governments, businesses, and consumers, and securing and protecting the privacy of our customers' and individuals' data are core drivers for our companies. Further, organizations across a variety of sectors often choose

¹ See ITI membership list at <http://www.itic.org/about/member-companies>.

to address risks to data and other cybersecurity risks today through the use of sophisticated third-party services providers, including some ITI companies, who offer innovative security technology, services, and risk management expertise, which may otherwise be lacking within those organizations. Consequently, ITI has been a leading voice in advocating for effective approaches to both privacy and cybersecurity.

I would like to begin my remarks by commending you, Chairman Luetkemeyer and Congresswoman Maloney, for the transparent and inclusive process through which you and your staffs have worked to develop this discussion draft. We share your goal of developing a uniform, preemptive, consumer protective data security and breach notification regime, and appreciate the openness with which you have not only listened to but considered our priority issues. Congress and the business community have worked for more than a dozen years to develop a regime that balances the concerns of all stakeholders, and this effort moves us closer to realizing that shared goal. We also recognize that compromises in this arena must be made, and we do not wish the perfect to be the enemy of the good. In that spirit of compromise, ITI supports many of the provisions in the discussion draft, but we also offer several recommendations aimed at further improving, refining, and clarifying the draft language.

I will focus the balance of my testimony on four areas: (1) the environmental backdrop and context calling for a streamlined federal data breach notification standard; (2) summarizing the positive principles reflected in the breach notification portion of the discussion draft; (3) assessing the security safeguards section of the discussion draft; and (4) offering recommendations to further improve, clarify, and refine the discussion draft.

Environmental Backdrop and Context

Our companies are not only data security solutions providers but are also stewards of sensitive customer data. As such, we have dual interests in seeing Congress adopt a federal data security

and data breach notification regime – both as third-party solutions providers and as covered entities. While companies across the digital ecosystem invest tremendous resources in defending their infrastructures, networks, and systems and protecting their customers' information, the defenders are engaged in an ongoing virtual arms race with attackers seeking to breach those systems and compromise that data. So, the reality facing organizations today is they must race to keep up with increasingly sophisticated and well-resourced hackers – ranging from criminals to nation-states – who are scheming to stay one step ahead of their victims. Unfortunately, the percentages do not favor the defenders, who must be successful every time to avoid a breach. Instead, the odds favor the attackers, who only need to be successful once to execute a successful breach. And when a breach of sensitive personally identifiable information (PII) occurs, we believe there should be a streamlined and uniform process to notify consumers in cases where there is a significant risk of identity theft, financial harm, or material economic loss.

There are currently 52 different breach notification regimes in 48 states and four U.S. territories.² And while there is no vacuum of consumer protection under this patchwork – consumers across the country have for years received notifications pursuant to these laws – the scope of legal obligations following a data breach is broad and complex because each of these notification laws varies by some degree, and some directly conflict with one another. The significant variances among these state and territory laws include the timeline for notification, the circumstances requiring notification, how notification should be effectuated, and what information should be included in a notification. Similarly, there is an expanding, convoluted patchwork of state data security laws. Today, there are more than a dozen laws regulating how data must be secured, ranging from requiring reasonable procedures appropriate to the

² The District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands each adopted a data breach notification law. South Dakota and Alabama have not yet enacted breach notification laws.

sensitivity of the data, to more prescriptive, compliance-based “check the box” approaches.³ Federal data breach notification legislation offers the opportunity to streamline the notification requirements into a single, uniform procedure, and to enhance the security landscape by incentivizing the adoption of security principles by entities in all 50 states that are flexible, risk-based, remain “evergreen,” and are adaptable to ever-changing threats.

Notification of Breaches Involving Sensitive PII

ITI has long advocated for federal data breach notification legislation that achieves the important goals of reducing consumer confusion, enabling faster consumer notification, and avoiding over-notification and consumer desensitization. ITI developed principles representing the elements a data breach notification bill must include to achieve these goals.⁴ The principles are attached to this testimony as Exhibit A. The discussion draft reflects the majority of these principles, including:

- Preempts the patchwork of existing laws and thereby reduces consumer confusion by ensuring consistency in notices, enables businesses to notify consumers faster than is possible under the patchwork of 52 different state and territory notification laws and avoids adding a 53rd standard to the inconsistent regulatory landscape;
- Creates an exception for information that is not in readable or usable form (such as via encryption);
- Recognizes the importance of avoiding over-notification by appropriately limiting the definition of “personal information” to data, which, if obtained by a criminal, could result in concrete financial harms;
- Recognizes that certain industries are already subject to breach notification requirements and does not impose an overlapping regulatory regime on those sectors;
- Allows notification to be effectuated by methods that are appropriate to each company-customer relationship;
- Recognizes the need for flexibility for companies and their third-party vendors to determine who should notify consumers in the event of a breach (consumers are often

³ Arkansas, California, Connecticut, Florida, Indiana, Kansas, Maryland, Massachusetts, Minnesota, Nevada, New Mexico, Oregon, Rhode Island, Texas, and Utah each adopted a law related to the security of personal information.

⁴ See <https://www.itic.org/dotAsset/e03b1f88-4661-4b5a-a105-6cc6df1eb028.pdf>

unaware of these third-party relationships and requiring a notification from the unknown third party to the consumer will create unnecessary confusion);

- Does not impose criminal penalties on victims of criminal hacks; and
- Recognizes both the danger of alerting hackers to vulnerabilities before they have been remediated (and risking potential further harm to consumers) and the risk of confusing or alarming consumers unnecessarily if companies are forced to notify prematurely – before a forensic investigation has been completed – under an arbitrary timeline. the discussion draft also permits companies to heed law enforcement requests to delay notification to allow for proper investigation of the incident or pursuit of criminal actors.

On balance, the breach notification section of the discussion draft offers much-needed regulatory clarity and certainty, which is critical for businesses that devote tremendous resources to data security and legal compliance.

Safeguarding Sensitive Personal Information

In the context of the data breach debate, the procedures often labeled “data security” are ultimately indistinguishable from risk management controls and best practices that are characterized as “cybersecurity” measures in other contexts. ITI has long advocated for the adoption and deployment of effective cybersecurity and data security measures by stakeholders across the digital ecosystem. ITI has actively participated in efforts to develop cross-sectoral, ecosystem-wide cybersecurity approaches grounded in sound risk management principles, international standards, and consensus best practices. ITI also supports efforts that are voluntary, leverage public-private partnerships, foster innovation in cybersecurity and data protection through their flexible application, and are scalable for organizations of all sizes and sophistication.

The threat landscape constantly evolves and so too must data protection and security measures. Any cybersecurity regulatory regime must complement – not replace – an organization’s existing risk management processes and program. Most importantly, ITI is a strong advocate of avoiding redundant or conflicting siloed approaches that complicate security

efforts for organizations and create inefficiencies by redirecting resources from securing their enterprise to static compliance programs. A company must be able to protect the information it holds in a manner that is reasonable and appropriate to the nature of its business and the sensitivity of the data it handles. The security program by which an organization chooses to secure data should be voluntary, based on effective risk management and provide companies with the ability to adapt rapidly to emerging threats, technologies, and business models.

The security safeguards section is consistent with a number of key security principles which, if followed in isolation, seem to provide effective guidance for an organization seeking to better protect information. For instance, § 3(a)(1) in the discussion draft calls for the development and implementation of “reasonable” security measures designed to protect the security of personal information from unauthorized acquisition, § 3(a)(2) calls for those safeguards to be flexible and appropriate to the particular size, resources and capabilities, and sensitivity of the data held by the covered entity, and § 3(a)(3) reflects the common elements of a risk management based approach to security, including core risk management functions such as Identify, Protect, Detect, and Respond. However, when considered as a whole, the security safeguards section is critically flawed in at least two respects.

First, the section creates a multi-layered set of requirements, setting forth a “reasonable security” standard in § 3(a)(1), and then prescribing a set of specific and in some cases rigid security requirements in § 3(a)(3). This structure exposes organizations to a regulatory “double jeopardy” of sorts, where they can employ all of the specific prescribed elements in § 3(a)(3) and yet still be found to have not implemented reasonable safeguards under the reasonableness standard in § 3(a)(1). We do not believe the bill should provide regulators with the unfettered discretion to decide whether “just” complying with the safeguards in §§ 3(a)(3)(A) through (E) is “reasonable enough.”

Second, § 3(a) (2) appropriately mandates that security safeguards be flexible, and appropriate to the particular characteristics of a covered entity, including its size, scope of business, available resources and security costs, and the sensitivity of the data it handles. Yet, § 3(a)(3) conflicts with this acknowledged need for flexibility. For instance, the requirement in § 3(a)(3)(A) that all covered entities designate a single employee to maintain safeguards ignores the fact that such a requirement might be completely inappropriate for a startup or small business, or even a larger organization that might choose instead to hire a service provider to provide managed security services.

In short, while the safeguards section gets much right in calling for organizations to adopt reasonable, flexible, and risk management-based approaches to security, it ultimately undermines its potential effectiveness in aspiring to require reasonableness and flexibility by also prescribing what that should look like in a sometimes rigid and inflexible manner, and ultimately providing regulators, rather than organizations, with the discretion to determine what security measures are reasonable.

Recommended Modifications

We appreciate that the discussion draft reflects a great number of our data breach notification priorities. Below, we offer several recommendations that will provide the business community with the clarity and certainty it requires in a regulatory regime that allows for the imposition of significant monetary penalties.

First, the timeline for notification should reflect the realities of completing an investigation and putting in place the apparatus necessary to notify very large numbers of consumers. An “immediate” notification is not only infeasible, it constitutes a bad security practice that puts consumers at risk of further harm if notification is required before vulnerabilities have been rectified, even if the “preliminary” investigation of the “who” and the “what” has been

completed. If vulnerabilities are not remediated before notification is triggered, consumers will undoubtedly be subject to further harm by would-be thieves who are alerted to the vulnerabilities by public notice. The discussion draft must allow companies to restore the reasonable integrity, security, and confidentiality of the data system *before* notifying consumers. Additionally, “immediately...and without unreasonable delay” are competing concepts – juxtaposing them as in the discussion draft is confusing and counterproductive. We recognize the urgency required for notification and recommend utilizing language from one of the existing state laws to convey such urgency. For instance, both New York and California require consumer notification “in the most expedient time possible and without unreasonable delay.”⁵

Second, the language under § 4(c)(1) that requires third parties to notify covered entities whose data “has or may have been compromised” must be amended to “has been compromised.” As drafted, § 4(c)(1) imposes an obligation on third parties to notify covered entities of breaches that “may have occurred” involving data that “may have been compromised.” This proposed requirement ignores the fact that cloud providers and other third parties deal with security incidents daily, ranging from minor to significant, often at very large volumes. These organizations cannot and should not be expected to notify customers based on a guess as to what “may” have happened. Further, the discussion draft imposes requirements on third parties who “suspect” a breach but have not confirmed it. Third parties frequently suspect breaches may have happened but upon investigation determine that no breach has occurred. These types of theoretical, rather than factual, inquiries would waste significant resources (of both third parties and covered entities) better devoted to implementing risk management controls or responding to actual compromises of data, lead to over notification, and serve no discernible purpose. We propose the discussion draft be amended to provide that third parties

⁵ N.Y. Gen. Bus. Law § 899-aa; Cal. Civ. Code § 1798.29.

should be required to notify only when hard evidence indicates that a compromise in fact occurred and resulted in exfiltration of the covered entities' data.

Third, the discussion draft must include a heightened burden of proof for regulators if the security measures remain layered by a reasonableness standard. Where a company complies with the enumerated elements of §3(a)(3), we recommend the Federal Trade Commission (FTC) or State Attorneys General be required to prove non-compliance with § 3(a)(1) – failure to “maintain reasonable administrative, technical, and physical safeguards” – through clear and convincing evidence. By mandating compliance with the enumerated safeguards under § 3(a)(3), the government mandates what a reasonable security program looks like and directs covered entities to focus on those specific practices. Where a company relies on the government’s directions, follows this mandate, and still suffers a security breach at the hands of a criminal hacker, it is reasonable to require the FTC or an Attorney General to demonstrate through additional proof that the company’s practices were nevertheless unreasonable. This heightened evidentiary standard would not render compliance with the enumerated safeguards optional, nor would it preclude the enforcement agency from finding that a company failed to implement reasonable safeguards; it would simply require a more thorough showing than a preponderance of the evidence by the FTC or an Attorney General that a company who complied with the enumerated safeguards nevertheless lacked reasonable safeguards.

Fourth, to clarify when a company will be considered a third party versus a covered entity, the definition of “covered entity” should be amended to read “any person, partnership, corporation, trust, estate, cooperative, association, or other entity that *owns or licenses* personal information.” As drafted, the definitions focus on the entity’s activity rather than the entity’s relationship to the data. Consequently, entities acting as third parties will in most if not all instances simultaneously be considered covered entities because both definitions use the verbs (or variants of the verbs) “accesses,” “maintains,” “stores,” and “handles” personal

information. This result is problematic because the discussion draft imposes different requirements on covered entities versus third parties, and the current overlapping definitions will in some instances cause third parties to be subject to both sets of divergent requirements for the very same activity. The proposed edits will clarify what is required of these entities in situations in which a breach of personal information they do not own or license occurs (when acting as third parties) versus what is required after a breach of personal information that they themselves own or license (as covered entities).

Fifth, the discussion draft permits unlimited civil penalties arising from a single incident. Most data breaches are the result of criminal acts, and breached entities are therefore the victims of a crime. Organizations can and should do their part to protect consumer data from unauthorized access, but uncapped civil penalties are seemingly punitive in nature and thus not appropriate to impose on an organization that has been victimized by criminal hackers or more sophisticated attackers, such as nation states. Further, data breaches are already extremely costly for companies, even before factoring in fines and penalties, when one considers the immediate response expenses of investigating and remediating the breach, notice to consumers and appropriate agencies, communications and media fees, reputational costs, loss of consumer trust, impaired goodwill, lost revenue, legal fees, and operational impacts. Any federal data breach law must contain reasonable penalty caps to avoid crippling fines that, on top of the myriad other reputational and response expenses, would risk putting companies out of business, including large publicly-traded companies who have a fiduciary duty to their shareholders. Further, the absence of reasonable penalty caps will make it much more difficult for companies to obtain cyber insurance – precisely the type of responsible behavior we should seek to advance through data security and breach notification legislation.

Sixth, the economic loss consideration in the risk standard should be amended to reference material economic loss. Without this clarification, companies would be liable for the most

minute of losses – for instance, the cost of a stamp to send a signed letter to a financial institution certifying one is not responsible for fraudulent charges is an economic loss – encouraging frivolous lawsuits that drain significant resources that are better invested in ongoing security risk management practices.

Seventh, the delay in notification permitted pursuant to a request by law enforcement – specifically by the U.S. Secret Service, the FBI, or State law enforcement – should be expanded to include requests by national security agencies such as the Department of Homeland Security or the National Security Agency, particularly given the rising number of incidents involving nation states, as well as the capacity of those agencies to render aid to companies that are victims of such attacks.

Eighth, the definition of “personal information” should be amended to exclude the words “alone or” in § 2(10)(A)(ii). Standalone financial account numbers in combination with merely a person’s name cannot be used to obtain credit, withdraw funds, or engage in financial transactions.

Ninth, substitute notice should be permitted in instances when notification will be required for greater than 1,000,000 individuals, or when notification will result in excessive cost to the organization. In either event, individual notification will result in draining resources that should more appropriately be committed to remediation of the vulnerability and continuing the capital-intensive efforts to secure personal information.

Conclusion

ITI and our member companies appreciate the Committee’s attention to this matter and its effort to develop a compromise solution to advance data breach legislation that provides for a single, rational federal breach notification standard, and incentivizes the adoption of

reasonable, flexible, risk-based data security practices. As ITI continues to gather feedback on the discussion draft of the *Data Acquisition and Technology Accountability and Security Act* 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 look forward to your questions.



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.

March 7, 2018

Statement for the Record

On behalf of the

American Bankers Association

before the

Financial Institutions and Consumer Credit Subcommittee

of the

Committee on Financial Services

United States House of Representatives



March 7, 2018

Statement for the Record
On behalf of the
American Bankers Association
before the
Financial Institutions and Consumer Credit Subcommittee
of the
Committee on Financial Services
United States House of Representative

March 7, 2018

Chairman Luetkemeyer, Ranking Member Clay, the American Bankers Association (ABA) is pleased to submit a statement for the record on the importance of enacting a uniform federal data breach law to protect consumers across the nation. The ABA is the voice of the nation's \$17 trillion banking industry, which is composed of small, mid-size, regional and large banks that together employ more than 2 million people, safeguard \$13 trillion in deposits and extend more than \$9.5 trillion in loans.

Protecting consumers in this increasingly sophisticated world of electronic commerce is a top priority of banks. It is clear that while our payments system remains strong, criminals continue to put consumers at risk by attempting to breach the security in almost every type of business and government agency. Banks and other financial institutions spend billions of dollars every year to protect consumers by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs. While the vast majority of payment card and other financial transactions are conducted safely, cyberattacks by criminals will continue against all businesses. If consumer financial information is stolen from retailers, businesses or banks, consumers have a right to swift, accurate, and effective notification of such breaches. They also should have confidence that, wherever they transact business electronically, the business is doing everything it can to prevent that breach from occurring in the first place.

Mr. Chairman, we strongly support your efforts to move forward on bipartisan data breach legislation. The ABA has consistently supported the following principles in legislation to provide stronger protection for consumer financial information:

1. Strong national data protection and consumer notification standards with effective enforcement provisions applicable to any party with access to important consumer financial information are critical. The costs of a data breach should ultimately be borne by the entity that incurs the breach.
2. Banks are already subject to robust data protection and notification requirements and that must be recognized.
3. In the event of a breach where consumers are at risk of harm, the public and other impacted parties should be informed as soon as reasonably possible.
4. State laws and regulations should be preempted in favor of strong Federal data protection and notification standards.

Banks are acknowledged leaders in defending against breaches. Therefore, from the financial services perspective, it is critical that data breach legislation takes a balanced approach that builds upon – *but does not duplicate or undermine* – what is already in place and highly effective in the financial sector.

The ABA is in the process of analyzing the Discussion Draft, and is likely to have further comments, but overall we are pleased that it addresses the critical goals that ABA members have advocated for many years and across several Congresses. ABA will continue to work with Congress to enact effective data security policies.

ABA would like to elaborate on the following points:

- **The need for a national data breach standard.** Consumers' electronic payments are not confined by borders between states. As such, a national standard for data security and breach notification is of paramount importance.
- **The importance of recognizing existing Federal breach requirements.** Any Federal data protection and notification requirement must recognize existing national data protection and notification requirements.

- **The ABA’s views on legislation.** Discussion Draft (the “Data Acquisition and Technology Accountability and Security Act”) and the “PROTECT Act of 2017.”

I. The Need for a National Data Breach Standard

Our existing national payments system serves hundreds of millions of consumers, retailers, businesses, banks, and the economy very well. Payments know no state border, nor does any cybercriminal. Therefore, a consistent national data breach policy is clearly necessary to effectively deal with the threats posed and protect customers.

Currently, 48 states, three U.S. territories, and the District of Columbia have enacted laws governing data security in some fashion, such as standards for data breach notification and for the safeguarding of consumer information. Although some of these laws are similar, many have inconsistent and conflicting standards, forcing businesses to comply with multiple regulations and leaving many consumers without protection and proper recourse. There is a better approach. Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification requirements. 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.

Given the mobile nature of our nation’s citizens, it is clear that the existing patchwork of state data breach laws are unduly complicated for consumers as well as businesses. For instance, consider a couple residing in a northern state who winter in a southern one and have their credit card data compromised at a merchant in a third state. In this instance, the couple wants to be alerted that their financial data has been compromised and that they are protected. Determining where the couple may or may not reside and which state laws may or may not apply unduly complicates the simple need to protect the couple from financial harm. It also diverts resources at the merchant and the bank toward determining how to comply with a myriad of laws as opposed to fixing the problem.

To limit the potential for data breaches in the first place, strong data protection requirements should be enacted that are applicable to any party with access to important consumer financial

information. Limiting the potential for such breaches through strong data protection is the first, essential, line of defense to maintain customer trust and confidence in the payments system.

Data security is also an ongoing process as opposed to the condition or state of controls at a point in time. Techniques of criminals change rapidly and prevention and mitigation efforts must as well. This is why ABA would oppose any mandated technology solution or specific security requirement which could soon become out of date and ineffective. A better approach, which is embodied in the Gramm-Leach-Bliley Act (GLBA) and the associated bank regulatory requirements, is to have a risk and governance-based approach rather than proscribing specific technological security requirements. Specifically, bank security programs are required to have “strong board and senior management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities.”¹ Such an expectation is national in scope and should be treated that way.

II. The Importance of Recognizing Existing Federal Breach Requirements

Any legislation on data breach must also take into consideration the fact that some industries – *including the financial industry* – are already required by law to develop and maintain robust internal protections to combat and address criminal attacks, and are required to protect consumer financial information and notify consumers when a breach occurs within their systems that will put their customers at risk.

Title V of the GLBA requires banks to implement a “risk-based” response program to address instances of unauthorized access to customer information systems. At a minimum, a response program must:

1. Assess the nature and scope of any security incident and identify what customer information systems and customer information may have been accessed or misused;

¹ Federal Financial Institution Examination Council IT Handbook, available at <http://ithandbook.ffiec.gov/it-booklets/information-security/introduction/overview.aspx>

2. Notify the institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information."
3. Notify appropriate law enforcement authorities and file Suspicious Activity Reports in situations involving federal criminal violations requiring immediate attention;
4. Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information, and
5. Notify customers "as soon as possible" if it is determined that misuse of customer information has occurred or is reasonably possible.

A critical component of the GLBA requirements is customer notification. When a covered financial institution becomes aware of a material breach of "sensitive customer information," it must conduct a reasonable investigation to determine whether the information has been or can be misused. If it determines that misuse of the information "has occurred or is reasonably possible," it must notify affected customers "as soon as possible."

Under GLBA, sensitive customer information includes the customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, credit card, debit card or other account number or personal identification number. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password.

A covered financial institution must also provide a clear and conspicuous notice. The notice must describe the incident in general terms and the type of customer information affected. It must also generally describe the institution's actions to protect the information from further unauthorized access and include a telephone number. The notice also must remind customers to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution.

Where appropriate, the notice also must include:

1. Recommendation to review account statements immediately and report suspicious activity;
2. Description of fraud alerts and how to place them;

3. Recommendation that the customer periodically obtain credit reports and have fraudulent information removed;
4. Explanation of how to receive a free credit report; and
5. Information about the FTC's identity theft guidance for consumers.

Banks that are engaged in the business of insurance marketing and sales face additional challenges with regard to data security because of the differences in the way banks and insurance companies are regulated. These differences can lead to duplicative and contradictory regulatory requirements for data security efforts.

Many financial institutions have affiliate agencies that can be housed in one of the three structures: in a bank itself, in a financial subsidiary of a bank, or in a nonbank subsidiary of a bank holding company (often a sister affiliate of the bank). Banks are heavily regulated with respect to the traditional products they offer – checking accounts, certificates of deposits, loans and lines of credit – so when it comes to data security, banks acting in their traditional roles must comply with a regulatory regime being established by banking regulators. Independent insurance agencies have their own set of rules they must follow, as established by state insurance regulators and that is the case for data security.

Consequently, when banks sell insurance – either directly or through an affiliated insurance agency – they face two different regulatory regimes: a regulatory regime that applies because they are banks, and a separate regulatory regime that applies because they are engaged in insurance. The current regulatory regime forces bank affiliated agencies to comply with contradictory regulatory requirements regarding data security. If an affiliate agency is operating in 48 states and a data breach takes place, the affiliate agency is forced to comply with 48 different data breach and notification standards as well as with federal regulatory requirements.

Within a bank holding company, cybersecurity is approached from the viewpoint of the entire holding company – not each affiliate individually. This is because the holding company may use a single information system for all of the affiliates within the holding company.

March 7, 2018

For these reasons, ABA recommends Congress pass legislation to allow data security and breach notification compliance by a bank holding company affiliate operating within the holding company's regulatory system (which satisfies all of the applicable bank regulatory requirements), to be deemed in compliance with federal law and to not be subject to duplicative regulation issued by state insurance authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act.

These are strong standards that the financial services industry already must comply with. As Congress contemplates data breach legislation, it is important that it build upon what is already in place and not duplicate or undermine what has already proven to be effective.

III. Discussion Draft, the “Data Acquisition and Technology Accountability and Security Act “

As mentioned at the outset, we strongly support Chairman Luetkemeyer and Representative Maloney's efforts to move forward on bipartisan data breach legislation. While we are still analyzing the full breadth of the Discussion Draft, we are pleased that it addresses the critical goals that ABA members have advocated for many years.

A. Data Protection

In particular, the data protection requirements in section 3 would put in place an effective data protection process for those that keep and use sensitive consumer information. Like the GLBA requirements that apply to financial institutions, every business must develop, implement and maintain reasonable administrative, technical and physical safeguards to protect sensitive personal information from unauthorized access and acquisition that is reasonably likely to result in identity theft, fraud or economic loss.

Also like GLBA, these safeguards must be appropriate to the size and complexity of the entity, the nature and scope of its activities, the cost of available tools to improve security and reduce vulnerabilities and very importantly, the sensitivity of the personal information it maintains. This makes implementing the safeguards a scalable and tailored process rather than a draconian, one-size fits all approach (which tends to hurt smaller businesses with fewer resources to draw upon).

The Draft provides guidance on what constitutes reasonable safeguards. For example, every company should delegate someone, either an owner, officer or employee, to oversee the safeguards that are put in place. The safeguards themselves are practical and basically what companies that are serious about data protection should be doing already. First, identify the internal and external security risks they face, and then implement safeguards designed to control those risks; ensure that any third parties they work with also protect the information; and evaluate and update everything as necessary for changes in technology and the threats to data security.

Any entity that obtains and uses a consumer's personal information should be required to protect it, no matter its size. However, there is no doubt that the approach taken in the Draft is flexible and depends on what information is obtained and how it is used. Despite arguments to the contrary, there is clearly no intent to apply rigid standards to businesses that do not keep and use significant amounts of sensitive personal information.

B. Breach Notification

ABA has consistently supported strong data protection in order to prevent breaches as the first, and best, line of defense. However, if a breach does occur, consumers should be informed of the nature and extent of any fraud, identity theft or other risks they may face, as well as guidance on what they can do to protect themselves. GLBA has put that standard in place for banks and for years our members have taken the brunt of dealing with the costs and other aspects of breaches at retailers and other companies when they involve payment card and other information.

In fact, most of the time the press releases and other public notices sent out by breached companies tell consumers to contact their bank or credit union to find out what they can do to protect themselves. Often, the first time customers learn of a problem is when a bank has to reissue his or her credit or debit card. Many customers get confused and believe that the card was reissued because of something the bank has done wrong rather than the retailer or business where the breach actually occurred. Banks try to explain what happened and most often without much information about the actual breach. And banks end up footing the bill for the cost of the card and other anti-fraud efforts.

That is why we strongly support the provisions in section 4 of the Draft that in most instances make the breached company responsible for notifying consumers about the breach as soon as possible after it determines the scope and extent of the breach. There still appear to be some grey areas that need to be worked out and we would be concerned if changes are made that could allow those that have the ability to contact and inform consumers about a breach to avoid that obligation.

There is one other major aspect of the notice requirements that we would address. The timing of the notice has, and continues to be, the subject of debate. Clearly, looking at it from the consumer side of the equation, and from the perspective of banks and others that might be impacted by a breach, notice should be provided as quickly as possible. However, it is also important to realize that every breach is different and that the exact scope of the breach, and exactly what personal information might have been put at risk, is generally not clear when a company first becomes aware that it has a problem. A certain amount of time and investigation is required to find out what happened and who should be notified.

In our view, it would be a mistake to put in place a time-certain for notification such as a certain number of hours or days. The standard set in the GLBA's requirements is "as soon as possible." While some states have specific maximum timelines, most are modeled on the GLBA standard although the exact language can differ. The reason for this is that consumers should be notified as soon as possible, but it is even more important that they are notified in a way that provides them with enough information to take effective action to protect themselves.

We think that the Draft attempts to balance this by providing that once the breached entity believes a breach of personal information may have occurred, it must conduct an immediate investigation to assess the nature and scope of the breach and take reasonable measures to restore security. After that, if there is a reasonable risk that the breach has, or could result in harm to the consumer the breached entity must notify law enforcement, appropriate regulators, consumers and other impacted entities "immediately and without unreasonable delay."

In addition, several safeguards are put in place such as a delay requested by law enforcement so that premature notification does not undermine the criminal investigation. There are also relatively low thresholds (5,000 or more consumers) for triggering notification to law enforcement, oversight agencies and the consumer credit reporting bureau. In addition, there is

guidance provided on the form of the notice and for how long the content must be kept available to consumers.

This timing language may require further discussion, but we would be very concerned if unrealistic timelines were to be added to the bill impacting financial institutions.

C. Oversight and Enforcement

One of the fundamental points ABA has strongly and consistently made is that banks are subject to oversight and examination for compliance with the GLBA data protection and notice requirements by several regulatory agencies. Depending on the bank's charter, the examinations are conducted by the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, or a combination of some or all of these agencies. It is more complicated than that, but what is clear is that every other bank in the country, has to prove it is in compliance with GLBA security and notice requirements and protecting our customers' data on a regular basis. There is no reason to duplicate that in another Federal law, and we are pleased that the Draft maintains that approach and leaves oversight and enforcement up to our prudential regulators.

With respect to non-banks, and certain financial institutions, the Federal Trade Commission (FTC) has historically had that oversight responsibility. The oversight of those companies is somewhat different than what we experience in that the FTC does *not* have examination authority. Instead, it relies on enforcing data protection requirements through consent orders after a breach has taken place. Section 5 of the Draft keeps that basic structure in place, but would also allow for the enforcement of the Federal data breach law by State Attorneys General.

D. Relation to State Law

As was mentioned earlier in this testimony, virtually every state has some sort of breach notification law in place, but only a small minority of states have enacted data protection laws. In our view, there needs to be a uniform standard for all states to better protect consumers and businesses across the nation. Our economy is nationwide, and in many cases global. It does not make sense to continue to address this issue through differing and often inconsistent state laws. It really should not matter where a consumer is located if their financial information has been compromised. A person living in one state should expect all businesses to respect and protect

March 7, 2018

their financial information and to notify them when breaches have occurred—protection that should be consistent regardless of what state in which someone resides.

The Draft addresses this problem by both putting in place a strong federal data protection requirement that applies nationwide, and preempting “any state law, rule, regulation, requirement, standard or other provision, with respect to securing information from unauthorized access or acquisition.” This makes sense from the perspective of the ABA and we would be concerned if this was not included in final legislation as it would amount to just another breach law on top of all the others already in place rather than real reform.

The legal, regulatory, examination and enforcement regime that is in place for banks ensures that banks robustly protect American’s personal financial information. We believe that the Discussion Draft provides an appropriate, scalable model for other businesses entrusted with sensitive customer financial and other information, and we strongly support your efforts to move forward on this important legislation.

Banks with affiliate agencies are often subject to oversight by the Office of the Comptroller of the Currency, the Federal Reserve, the FDIC, state banking regulators and state insurance regulators. The different regulatory regimes cause banks with affiliate agencies to be faced with contradictory regulatory requirements regarding data security and breach notification. ABA strongly supports a bank holding company affiliate operating within the holding company’s regulatory system (which satisfies all of the applicable bank regulatory requirements), to be deemed in compliance with federal law and to not be subject to duplicative enforcement by state regulators.

IV. The PROTECT Act of 2017 (H.R. 4028)

Our understanding is that this bill has three basic parts and we have a few brief comments on each. Title I provides for the supervision and examination of large consumer reporting agencies by at least one of the Federal banking agencies. Although the data security standards of the GLBA apply to the credit bureaus, and they are subject to the FTC’s oversight, they do not undergo rigorous bank-like examinations. Given the size of these organizations and the sensitivity of the information they keep, it would make sense for the Committee to consider this

to better protect sensitive consumer information. ABA members would be concerned if this were to create additional compliance burdens on banks, but as far as we can tell this does not seem to be the case with respect to the provisions currently in the bill.

Title II would put in place various requirements that allow consumers to freeze, unfreeze and temporarily lift a credit freeze on their credit. Consumers are given a great deal of flexibility in how they make these requests and the credit bureaus have to meet certain time limits in implementing them. In the case of identity theft victims, active duty military, minors and senior citizens, they are free of charge. For others, a low fee can be charged. Overall, we do not see major problems if this were to be put in place. However, in experiences shared with us by bankers it could have an impact on the availability of credit for consumers that do not actively manage their frozen accounts.

Title III would prohibit the national credit bureaus from using social security numbers (SSNs) after January 1, 2020 in consumer reports, as a method for identifying a consumer and “for any other purpose.” While we recognize that there is great concern about the use of stolen SSNs in general, and in particular with respect to the creation of synthetic “IDs,” it is just not feasible to do this at this time for a number of reasons. The government and private sector use SSNs extensively, and an equivalent personal identifier does not exist. Thus, prohibiting the use of SSNs would (1) increase the potential for identity theft, (2) increase the cost not only of credit but other banking products, and (3) reduce the availability of credit and other banking services, all to the detriment of consumers. Creating a new, universal personal identifier and replacing the SSN cannot be achieved in the short time the bill demands. Moreover, whatever replaces the SSN simply becomes the new target with the same problems.

Our suggestions are to conduct a study of how and why SSNs are currently used by both the private sector and government and to identify ways to reduce their misuse and other options for verifying people’s identity.

Conclusion

We appreciate the opportunity to present our views on both the Discussion Draft and the PROTECT Act, and we look forward to working with you and the Members of the Committee on this important legislation.



March 6, 2018

The Honorable Blaine Luetkemeyer
 Chairman
 Committee on Financial Services
 Subcommittee on Financial Institutions and
 Consumer Credit
 U.S. House of Representatives
 2230 Rayburn House Office Building
 Washington, D.C. 20515

The Honorable Lacy Clay
 Ranking Member
 Committee on Financial Services
 Subcommittee on Financial Institutions and
 Consumer Credit
 U.S. House of Representatives
 2428 Rayburn House Office Building
 Washington, D.C. 20515

Dear Chairman Luetkemeyer and Ranking Member Clay:

The Consumer Bankers Association (CBA) writes to comment on the March 7th, 2018 Subcommittee hearing, entitled "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime." In particular, CBA supports the "Data Acquisition and Technology Accountability and Security Act" to establish a national data security and breach notification standard and we look forward to making improvements to the bill throughout the legislative process. CBA is the voice of the retail banking industry whose products and services provide access to credit to millions of consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans and collectively hold two-thirds of the country's total depository assets.

The Data Acquisition and Technology Accountability and Security Act

CBA supports the Data Acquisition and Technology Accountability and Security Act discussion draft to help protect consumers' sensitive information throughout the payment system by establishing a national data security and breach notification standard. Importantly, the discussion draft recognizes banks and credit unions already adhere to strong security controls and notification requirements and are supervised by their prudential regulators for compliance with such standards. This needed legislative proposal applies a similar, scalable standard to retailers and other sectors to better protect consumers' sensitive information and require timely consumer notification in the event of a breach. The discussion draft also provides preemption from the existing patchwork of state laws and allows for the enforcement of the new standard by the Federal Trade Commission and states' Attorneys General. This discussion draft is an important step forward and CBA commits to working with the sponsors and other stakeholders to enact legislation to help safeguard consumers from future breaches.

The Promoting Responsible Oversight of Transaction and Examinations of Credit Technology Act of 2017

The Promoting Responsible Oversight of Transaction and Examinations of Credit Technology Act of 2017 (H.R. 4028) brings needed attention to cyber threats and the seriousness of having in place effective data security protocols. Today, financial institutions are subject to data security and notification requirements under the Gramm-Leach-Bliley Act. While banks and credit unions are subject to supervision and enforcement by their prudential regulators for compliance with these safeguards, non-depository financial institutions are only subject to enforcement by the Federal Trade Commission. H.R. 4028 recognizes this void in the current compliance regime

and places nationwide credit reporting agencies under the supervision of a prudential regulator as determined by the Federal Financial Institutions Examination Council.

CBA recognizes many consumers are seeking ways to ensure the security of their personal data and more closely monitor their credit reports. Our members are committed to making sure customer data is safe and secure and spend considerable resources on fraud monitoring and resolution.

While CBA members understand the intent of H.R. 4028 to provide quick and affordable access to credit freezes in light of recent breaches, there could be potential unintended consequences to consumers' on-demand access to credit. Today, consumers expect real-time credit approvals, and any delays can be confusing and frustrating. While credit freezes may be the appropriate choice for some consumers, others may prefer options that enable on-demand access to credit. Given the potential negative implications of this section on the availability and flow of credit, we encourage further debate on this important topic prior to passing legislation changing the current credit reporting structure.

In addition, this legislation would prohibit the use of a Social Security Number (SSN) as consumer report identifier past January 1, 2020. More can and should be done to protect consumers' identities, but a deviation from the widespread use of the SSN as the primary identifier to a new and untested alternative could cause unintended harm and impede the flow of credit to consumers. CBA looks forward to working with Congress, regulatory agencies, and other participants in the credit markets to discuss and study alternatives that would help protect consumers from criminals seeking to steal their identities.

Thank you for the opportunity to comment on these legislative proposals. We look forward to working with the Subcommittee to ensure the security of consumers' sensitive information while providing robust and healthy credit markets.

Sincerely,



Richard Hunt
President and CEO
Consumer Bankers Association



March 6, 2018

Chairman Blaine Luetkemeyer
 Ranking Member William Lacy Clay
 Subcommittee on Financial Institutions and Consumer Credit
 2129 Rayburn House Office Building
 Washington, DC 20515

Re: Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime

Dear Chairman Luetkemeyer and Ranking Member Clay,

On behalf of the Center for Democracy and Technology (CDT), we write regarding the draft Data Acquisition and Technology Accountability and Security Act. We appreciate Congress' interest in securing Americans' data and want to share the following concerns with the the bill as drafted. We believe that, without amendment, the bill would harm the security and privacy of consumers. Our primary concerns are as follows:

- The definition of "personal information" protected by the bill is far too narrow. The bill only covers information accompanied by first name or initial and last name in the prospective security requirements and breach notification obligations. This definition does not reflect the practical ways in which personal data is used by commercial entities nor is in line with the last several decades of federal and state privacy policy and law.¹ As the bill explicitly notes, other identifiers like social security numbers, account numbers and biometrics are frequently used to "authenticate an individual's identity," and "obtain money, [and] purchase goods." Further harms from breaches of personal information extend to other areas not covered by the legislation such as intimate photos or personal communications.
- Including a trigger based on economic harm disregards real life consequences of breaches. Requiring a nexus of identity theft, fraud or economic loss for notification to kick in does not recognize the breadth of consequences that may result from a breach including harassment, stalking, loss of access to online accounts, and reputational harm. Nearly all state and federal laws and policy on data breach recognize that monetary loss is just one possible impact on an individual, and that other sensitive data must be protected too. The bill also requires notification to consumers only *after* the breached entity determines that the breach "has resulted" in identity theft, fraud or economic loss, impeding any effort on the part of the consumer to forestall these harms in the first place. A wholistic and forward-looking approach to breach

¹ See the definition of "personally identifiable information" used by federal agencies, which includes "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." Additionally, most state laws include categories of information that is protected regardless of its nexus to a name. See https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.



notification must recognize that far more is on the line for consumers than just dollars and cents.

- Bottlenecking enforcement in a single court and a single federal agency will undercut any security benefits of the bill. As drafted, consumers are barred from seeking any judicial redress for the breach of their personal information. State attorneys general will have their actions consolidated into the US District Court for the District of Columbia--where a typical civil trial averages three years from start to finish²--and will be precluded from protecting the rights of their constituents altogether if the Federal Trade Commission opens an investigation. Even if Congress intends to usurp states' rights to set their own security standards, the FTC does not have the authority, resources or staff capacity to effectively and single-handedly absorb responsibility for cybersecurity enforcement writ large.
- Exempting entities covered by the Gramm-Leach Bliley Act means financial institutions would not be required by law to notify consumers of data breaches. Guidelines on the GLBA are developed by federal agencies, such as the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation. These guidelines do not explicitly require financial institutions to develop a data breach response plan nor are they required to notify consumer even when they are aware that stolen personal information has been misused. Entities like Equifax, responsible for last year's unprecedented breach of personal information for 145.5 million Americans, would not be subject to the bill as written.

Cybersecurity legislation of general applicability must demand more from those who choose to collect and keep sensitive data. Poor cybersecurity practices have led to a data breach crisis affecting consumer rights, corporate stability, critical infrastructure and the country's national security. As drafted, this legislation would eliminate strong existing state protections, while replacing them with a federal standard that is sharply limited in both what types of information it protects and how consumers are notified in the case of breaches.

Thank you and we look forward to working with you to refine the bill.

Sincerely,

Michelle De Mooy
Director, Privacy and Data Project

Michelle Richardson
Deputy Director, Freedom, Security and Technology Project

² U.S. Administrative Office of the Courts, <http://www.uscourts.gov/report-name/judicial-facts-and-figures>.

March 7, 2018

The Honorable Blaine Luetkemeyer
Chairman, Subcommittee on Financial
Institutions and Consumer Credit
House Committee on Financial Services
Washington, DC 20515

The Honorable Lacy W. Clay, Jr.
Ranking Member, Subcommittee on Financial
Institutions and Consumer Credit
House Committee on Financial Services
Washington, DC 20515

RE: Hearing on "Legislative Proposals to Reform the Current
Data Security and Breach Notification Regulatory Regime"

Dear Chairman Luetkemeyer and Ranking Member Clay,

The undersigned associations, representing over a million businesses in industries that directly serve American consumers, sent a letter to you on February 13, 2018, laying out four critical principles that any federal legislation on data security and breach notification should meet. These include establishing a nationwide law, setting data security standards reasonable and appropriate for the covered businesses, maintaining an appropriate enforcement regime, and ensuring all breached entities have notice obligations.

With these principles in mind, we have reviewed the draft legislation that Chairman Luetkemeyer and Representative Carolyn Maloney have circulated. We have some significant concerns regarding this draft as set forth in greater detail below:

- **Breach Notice:** The draft bill does not ensure that *all* breached businesses have obligations to investigate and provide notice to regulators and consumers of their breaches. Instead, the draft carves out exceptions from notice for three categories of businesses: "third parties;" "service providers;" and a large category of financial institutions. For example, the bill creates an exemption for "service providers" that is not found in any state breach notification laws but, as defined, could apply to virtually any third-party service that handles data. The draft bill does not require "service providers" to even investigate the nature and scope of a suspected data breach, ensuring they will never *know* whether personal information is acquired in their breaches of security. Consequently, these breached businesses will never have to notify anyone at all. Exempting businesses from investigatory and notice obligations and, in some cases, requiring other businesses to undertake those notice obligations for them, is fundamentally unfair and undermines data security efforts in the U.S. Exempted business will have reduced incentives to protect data if they are not required by federal law to shine a light on their breaches. The fact that the draft legislation gives these exempted businesses preemption from any states that might want to require them to provide notice under state laws would effectively shield these breached businesses from *ever* disclosing their breaches.

- **Data Security:** The draft legislation sets data security requirements that are unreasonable and inappropriate for millions of commercial businesses. Mandating a checklist of specific requirements that all businesses must meet to comply with a federal data security statute does not work for the millions of diverse businesses across the nation that will be subject to prescriptive obligations inappropriate for the nature of their operations. These businesses vary tremendously in size, complexity, sophistication, the type of data they touch and the volume of data they exchange. According to data security experts who have testified before Congress in recent years, effective data security standards use a risk-based approach applying the highest security standards to the most sensitive data at the greatest risk. A one-size-fits-all standard misses the mark on this critical point. The draft legislation itself seems to partially recognize this problem by exempting financial institutions from its data security requirements, but doesn't fully recognize it because the bill also applies security requirements designed for banks onto businesses with less sensitive data. Rather than establishing a check list, the bill should employ, as the Federal Trade Commission (FTC) does, a flexible, reasonable standard for data security that could be applied appropriately to each kind of business handling personal information.
- **FTC Enforcement:** The draft legislation modifies the FTC's traditional enforcement powers so that its actions can be punitive and the Commission could exact fines *even before* the specifics of the data security standards it is applying have been established. That breaks with over one hundred years of agency enforcement practices and means that businesses could be fined that could not have known what they were required to do to avoid those fines. The bill should maintain an appropriate FTC enforcement regime consistent with the agency's long-standing traditions.

The above are a few of the fundamental concerns we have with the approach to data security taken by the draft legislation. We also have concerns that the legislation: sets an "immediate" standard for notice which is not a legal standard we have seen employed and may be unachievable; does not allow practical ways for breached systems to be secured or for law enforcement to seek a delay prior to requiring public notice to be given; requires notice in states where the breached business may not be aware any affected consumers reside; inappropriately requires notice to private businesses as though they are federal regulators; and allows financial institutions to provide their customers with inaccurate information in the event of a breach.

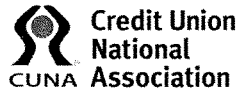
In light of these many concerns and the importance of this issue, we strongly urge you to take the time to fully consider all of these and other issues with the draft and work through them with stakeholders prior to moving to a markup. We appreciate the process and consideration that Chairman Luetkemeyer and Congresswoman Maloney have given to these issues to date, and believe more discussion and work is needed to produce legislation that will be effective and fair.

We appreciate your consideration of our views and we look forward to a continued constructive dialogue with you on these matters.

Sincerely,

International Franchise Association
National Association of Convenience Stores
National Association of Truck Stop Operators
National Council of Chain Restaurants
National Grocers Association
National Restaurant Association
National Retail Federation
Petroleum Marketers Association of America
Society of Independent Gasoline Marketers of America
U.S. Travel Association

cc: Members of the U.S. House of Representatives



Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601

March 7, 2018

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions and
Consumer Credit
United States House of Representatives
Washington, DC 20515

The Honorable William Lacy Clay
Ranking Member
Subcommittee on Financial Institutions and
Consumer Credit
United States House of Representatives
Washington, DC 20515

Dear Chairman Luetkemeyer and Ranking Member Clay:

On behalf of America's credit unions, I am writing regarding today's hearing titled "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime." The Credit Union National Association (CUNA) represents America's credit unions and their 110 million members.

Last month, Kim Sponem, President and CEO of Summit Credit Union testified on behalf of CUNA before the subcommittee on this critical issue. We appreciate efforts by Chairman Luetkemeyer and Rep. Maloney to advance draft data breach legislation that contains the principles CUNA's witness stated should be part of any legislation. The principles include:

- A flexible, scalable data protection standard;
- A notification regime requiring timely notice to impacted consumers, law enforcement and applicable regulators;
- Enforcement of the new national standard by the Federal Trade Commission and state attorneys general;
- Does not exclude a private right of action; and,
- Clear preemption of the existing patchwork of often conflicting and contradictory state laws

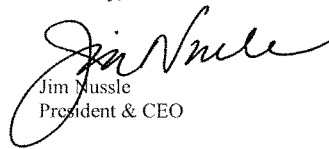
We appreciate the Subcommittee's continued focus on this important issue. Data breaches have harmed and will continue to harm credit unions and their members. These breaches have exposed personally identifiable information (PII), including Social Security numbers, birth dates, driver's license numbers, and payment card data including credit and debit card numbers. As such, hackers have had access to highly sensitive PII and payment card data exposing credit unions to damages in replacing members' payment cards, covering fraudulent purchases, and taking protective measures to reduce risk of identity theft and loan fraud and assuming financial responsibility for various types of fraudulent activity related to stolen identities and misuse of PII and payment card data.

In addition to Equifax, big box retailers, other merchants, and insurance companies have all been breached in recent memory. And the risk is not limited to the private sector; many in Congress will recall significant breaches in recent years of personal information at the Office of Personnel Management and the Internal Revenue Service.

As this Subcommittee works to shed light on the impact of the data breaches and to ensure consumers are not at further risk, we encourage you and your colleagues to consider the risk to consumers' personal data in other sectors of the economy, including the retail sector, as well as at federal agencies.

On behalf of America's credit unions and their 110 million members, thank you for holding this hearing. We look forward to working with you on this important issue.

Sincerely,



Jim Mussle
President & CEO



March 7, 2018

DATA SECURITY LEGISLATIVE SOLUTIONS: THE COMMUNITY BANK PERSPECTIVE

On behalf of the nearly 5,700 community banks represented by ICBA, we thank Chairman Luetkemeyer, Ranking Member Clay, and members of the Financial Services Subcommittee on Financial Institutions and Consumer Credit for convening today's hearing on "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime." ICBA is pleased to have the opportunity to submit this statement for the hearing record.

Community banks are committed to safeguarding customer data and personal information. The community bank business model is founded on customer trust and service. Data security is a business imperative in the digital marketplace. Community banks invest significant and increasing resources in security controls to protect their consumers' data and critical systems.

ICBA is pleased to offer the community bank perspective on the two legislative proposals before this committee today.

THE "DATA ACQUISITION AND TECHNOLOGY ACCOUNTABILITY AND SECURITY ACT"

This discussion draft, offered by Chairman Luetkemeyer and Rep. Carolyn Maloney, would create a national data breach notification standard to replace the current patchwork of differing state breach notification laws. In an integrated national economy with a geographically mobile population, consistent standards and expectations are needed to avoid consumer confusion.

ICBA supports the security requirements in the discussion draft, which would subject other entities to a scalable data security standard. Community banks have long been subject to regulatory mandates that set rigorous data protection practices. These mandates are fundamental and a critical component of the safety and soundness of the overall banking system. With data breaches in the news almost daily, the status quo advocated by other sectors is simply not working for American consumers. Consumers demand that their personal information be held securely and not subject to innumerable breaches. The only way to achieve this objective is by raising the bar to ensure all entities are subject to comparable standards.

While ICBA is supportive of the discussion draft and the objectives it is attempting to achieve, we respectfully recommend that the bill be strengthened by creating incentives for improved data security for all entities that hold, store, or process personally identifiable information by creating a legal structure in which the entity that incurs a breach – be it a retailer, credit reporting agency (CRA), or other entity – bears financial liability for the cost of the breach.

When a breach occurs at any point in the financial services chain, community banks take a variety of steps to protect the integrity of their customers' accounts, including, among other things, monitoring for indications of suspicious activity, changing customer identity procedures, notifying customers, responding to customer inquiries, reimbursing customers for confirmed fraudulent transactions, modifying customer limits to mitigate fraud losses, and blocking and reissuing payment cards of affected account holders at a cost to the community bank. Deposit account-holding and payment card-issuing banks repeatedly bear these costs up front because prompt action following a breach is essential to protecting the integrity of customer accounts. But these costs should ultimately be borne by the entity that incurs the breach. This is not only a matter of fairness; a liability shift is needed to properly align incentives for entities that store consumer financial and personally identifiable data to strengthen their data security. When breaches have a material impact on entities' bottom line, they will quickly become more effective at avoiding them.



ICBA thanks Chairman Luetkemeyer and Rep. Maloney for crafting this proposal, and we look forward to working with them as it advances.

THE “PROMOTING RESPONSIBLE OVERSIGHT OF TRANSACTION AND EXAMINATIONS OF CREDIT TECHNOLOGY ACT OF 2017” (H.R. 4028)

H.R. 4028, sponsored by Rep. Patrick McHenry, would, among other things, subject the CRAs to examination and supervision by a banking regulator to be determined by the Federal Financial Institution Examinations Council (FFIEC). ICBA strongly supports Title I of this bill.

The massive data breach at Equifax, which exposed the personal data of 148 million American consumers and counting, shows the ongoing vulnerability of CRAs. While CRAs are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA), they are not examined or supervised for their compliance with these standards in the same manner as financial institutions, yet they hold equally critical, personally sensitive information about consumers. This is a grave weakness in our current system. Significant third-party vendors that serve financial institutions are already subject to examination and supervision for compliance with GLBA standards. By the same logic, CRAs should be examined and supervised by the prudential financial regulators.

ICBA thanks Rep. McHenry for introducing H.R. 4028 and we look forward to working with him as it advances through the legislative process.

CLOSING

Thank you again for convening today's hearing. Data breaches are among the highest concerns of America's community bankers. ICBA looks forward to continuing to work with the committee to enact laws that will promote customer security, protect against costly and damaging data breaches, and further enhance the safety and soundness of our financial system.



March 7, 2018

The Honorable Blaine Luetkemeyer
 Chairman
 House Committee on Financial Services
 Subcommittee on Financial Institutions
 and Consumer Credit
 Washington, DC 20510

The Honorable William Lacy Clay
 Ranking Member
 House Committee on Financial Services
 Subcommittee on Financial Institutions
 and Consumer Credit
 Washington, DC 20510

**RE: Hearing on “Legislative Proposals to Reform the Current Data Security and Breach Notification
 Regulatory Regime”**

Dear Chairman Luetkemeyer and Ranking Member Clay,

The National Association of Convenience Stores (“NACS”) represents the convenience and fuel retailing industry, which employs approximately 23 million workers who serve around 160 million customers per day at over 150,000 stores across the United States. The industry, however, is truly an industry of small businesses. Approximately 63 percent of convenience store owners operate a single store, and approximately 74 percent of our membership is composed of companies that operate ten stores or fewer.

NACS supports the enactment uniform data breach notification legislation requiring businesses in all industries to notify their customers of data breaches that could cause them financial harm if that legislation improves upon current law. To be effective, federal data security and breach notification legislation should apply nationwide, set reasonable data security standards, maintain an appropriate enforcement regime, and ensure that all breached entities have notification obligations, regardless of industry. We are concerned that the draft legislation released by Chairman Luetkemeyer and Representative Carolyn Maloney weakens current law by creating exemptions that will keep some industries’ data breaches secret from regulators and/or the public.

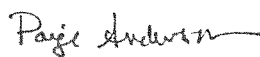
First and foremost, the draft bill does not impose notice requirements on some businesses. Rather, the draft bill carves out exceptions for a substantial number of financial institutions, as well as so-called “third parties” and “service providers.” In some cases, the draft bill would not only exempt such businesses from notice requirements; it would require other businesses to shoulder notice obligations for them. This is deeply unfair, and would ultimately undermine—rather than bolster—data security by reducing incentives for carved-out entities to protect their data. The fact that the draft legislation would preempt state notice laws with respect to carved-out businesses compounds this problem. This means the draft bill would substantially weaken current law. Data

breaches in some sectors – such as telecommunications – could run rampant and Americans would be completely unaware of that fact. That risk is heightened by the fact that the “service provider” definition in the draft bill is vague and many businesses might claim they qualify as “service providers” and avoid any obligation to investigate their data breaches or provide notice of them.

NACS shares many other concerns regarding the draft bill and detailed some of these concerns in a separate letter sent along with a coalition of industry groups. But, we wanted to emphasize this one area in a separate letter. If legislation locks in exemptions from data breach notification for certain industries, we are bound to weaken our national data security and be caught unaware by the insecurity of our data. We will have fraud without any idea from whence it came and be without the information to make improvements in the future. Secret breaches cannot be the result of good legislation.

Thank you for taking NACS’s views into account and your willingness to work with us to date. We urge you to continue working with interested groups on the draft bill to improve it before moving to a markup. We would be pleased to continue to work with you toward that end.

Sincerely,

A handwritten signature in cursive script that reads "Paige Anderson".

Paige Anderson
Director, Government Relations
National Association of Convenience Stores

cc: Members of the U.S. House Committee on Financial Services



3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Wm. Lacy Clay
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
U.S. House of Representatives
Washington, D.C. 20515

March 7, 2018

Re: Hearing on "Legislative Proposals to Reform the Current Data Security and Breach Notification Regime"

Dear Chairman Luetkemeyer and Ranking Member Clay:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today in conjunction with today's hearing on data security to share our thoughts on the broader topic and the specific bills before you today. We appreciate the Subcommittee's continued focus on this important topic and need for addressing consumer data security issues. As NAFCU testified before the Subcommittee last November, there is a need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements as depository institutions. We are pleased to see the Subcommittee is continuing its work on this important topic.

NAFCU's Principles on Data Security

As our testimony noted, we recognize that a legislative solution is a complex issue, and thus have established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.
- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the *Gramm-Leach-Bliley*

Act (GLBA), credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if those criteria are not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on depository institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.
- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the negligent entity who incurred the breach.

The Data Acquisition and Technology Accountability and Security Act

NAFCU is pleased to see the draft legislation proposed by Chairman Luetkemeyer and Representative Maloney which would establish a national standard for both data security and breach notification, while recognizing the existing framework from the GLBA that has been in place for financial institutions for nearly two decades. We also appreciate that the legislation maintains the status quo on the ability of credit unions to take a private right of action to recoup costs suffered in a data breach.

As the Subcommittee examines the discussion draft, we would encourage you to clarify and

make improvements to the draft. For example, in Section 4 dealing with notification, the timeline for notice to consumers is “immediately notify without unreasonable delay,” which could lead to confusion and may interfere with law enforcement efforts. We believe timely notification is critical, but would urge greater clarity of this provision. We would also like to see greater clarity on the requirements to provide timely notification to financial institutions holding accounts of consumers who have been victims of a data breach.

We also believe that there should be some technical fixes and clarity in Section 5 to ensure that credit unions that are bound by GLBA are deemed in compliance with the data security requirement in Section 3 and the breach notice requirement in Section 4. We believe that this is the intent of this section, but believe it is unclear if the proposed language would accomplish that.

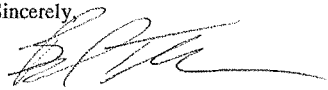
NAFCU is supportive of the efforts with this legislation and we stand ready to work with you on this bill as it moves forward in the legislative process.

H.R. 4028, the *Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017*

NAFCU is supportive of Title I of H.R. 4028, the *PROTECT Act of 2017*, offered by Representative McHenry, which would subject large consumer reporting agencies to supervision and examination by the Federal Financial Institutions Examination Council (FFIEC). This would help address some of the concerns about the gaps in regulation of large credit rating agencies. While we believe there could be merit behind the proposals in Title II to establish a system for a national security freeze and Title III’s phase-out of the credit rating agency use of Social Security Numbers, we believe these topics need further study for potential broader impacts and to avoid unintended negative results.

On behalf of our nation’s credit unions and their more than 110 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information please contact me or Allyson Browning, NAFCU’s Associate Director of Legislative Affairs, at 703-842-2836 or abrowning@nafcu.org.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Financial Institutions and Consumer Credit



STATEMENT OF

DAVID FRENCH
SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS
NATIONAL RETAIL FEDERATION

FOR THE

HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

HEARING ON

“LEGISLATIVE PROPOSALS TO REFORM THE CURRENT DATA SECURITY
AND BREACH NOTIFICATION REGULATORY REGIME”

MARCH 7, 2018

National Retail Federation
1101 New York Ave., NW
Washington, DC 20005
(202) 783-7891
www.nrf.com

EXECUTIVE SUMMARY

Our full statement appears in the following pages, but the key elements of our statement may be summarized as follows:

- 1. Breaches occur everywhere. All businesses should have breach disclosure requirements.**
 - Breaches occur most often where very sensitive data that is highly valuable to thieves can be acquired, such as from financial institutions and the government.
 - According to the *2017 Data Breach Investigations Report*, published by Verizon, the financial services sector suffers about one-quarter of all breaches annually. This study examines *where* breaches occur, not just which businesses *report* breaches – an important distinction considering that not all industries are required to report their breaches.
 - Any comprehensive federal legislation should therefore require all financial institutions and other businesses to disclose breaches of sensitive data when they occur.
- 2. Under today's banking laws, financial institutions can keep their data breaches secret.**
 - The Gramm-Leach-Bliley Act of 1999 predates the first state breach notification law by three years and does not require financial institutions to provide notice of their breaches.
 - Regulatory guidance issued in 2005 to interpret the law also does not require financial institutions to make data breach disclosures, leaving disclosure to their discretion.
 - The proposed legislation deems financial institutions' *discretionary* guidance regime as meeting the bill's *mandatory* requirement for covered entities to disclose breaches.
 - The Committee should fix this "notice hole" in its breach legislation moving forward.
- 3. Data security requirements should be reasonable and appropriate for each business.**
 - Mandatory requirements to protect sensitive information should take into account the nature of the business being regulated, the sensitivity of the data it handles, and the extent to which it processes, or engages in transactions with, the most sensitive information.
 - "One-size-fits-all" data security regulation, as proposed in legislation, is not appropriate for the vast array of American businesses to be covered. This bill would place mandatory security requirements on all businesses that were designed for financial institutions with \$10 billion or more in assets and handling the most sensitive financial information.
 - Retailers support legislation embodying a risk-based approach recommended by security experts and already adopted by the Federal Trade Commission (FTC). The FTC has brought more than fifty actions against businesses that fail to protect data at the level reasonable and appropriate for that business and the sensitivity of the data they handle.
- 4. Improving the security of payment cards themselves would help reduce card breaches.**
 - If banks issued Chip-and-PIN cards in the U.S. as they do globally, the incentive for hackers to steal card data and the number of breaches would be dramatically reduced.
 - New EMV chip-and-*signature* cards do not stop lost or stolen card numbers from being used online or in stores, so the incentive for criminals to steal card numbers remains.
 - If U.S. banks required PINs to approve transactions, as they do around the world, card numbers could be rendered useless to would-be thieves, reducing their incentive to steal.
 - Like ATM transactions, requiring PIN-level security for credit and debit card purchases should be part of any comprehensive solution addressing data breaches.

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee on Financial Institutions and Consumer Credit, on behalf of the National Retail Federation (NRF), I want to thank you for the opportunity to respectfully submit this statement for the hearing record and provide you with our views on legislative proposals to reform the current data security and breach notification regulatory regime, including the discussion draft of the “Data Acquisition and Technology Accountability and Security Act” circulated for stakeholders’ review in February (“Discussion Draft”). Cybersecurity threats face every sector of the U.S. economy, and NRF supports comprehensive and achievable legislative solutions that Congress and the White House may work toward to better protect Americans’ sensitive financial and personal data.

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.

A. Introduction

We appreciate the Subcommittee calling this hearing at a time when many kinds of American businesses find themselves the targets in an evolving war on our digital economy – a war in which they are unwilling combatants who must defend vigorously against attacks by both criminals and nation states. Key aspects of the cyberattacks facing the breadth of American industry sectors are, typically, the criminal fraud motive and the foreign source of the attack. Virtually all the data breaches we have seen in the United States during the past few years – from attacks on the networked systems of technology, retail, and entertainment companies that have been prominent in the news, to a reported series of attacks on our largest banks – have typically been perpetrated by overseas criminals who are breaking U.S. laws. These breached companies are victims of these external actors’ crimes, and we should keep this in mind as we explore the issues discussed at the hearing and in forthcoming public policy initiatives related to this issue.

Retailers collectively spend billions of dollars safeguarding sensitive customer information and fighting fraud that results when criminals succeed in breaching their protected information systems. Data security is at the top of retailers’ business priorities, and securing data from increasingly sophisticated attacks is an effort that our member companies, as a retail community, strive to improve every day. Data security is also an issue on which the retailer and consumer interests are aligned in the effort to protect the most sensitive information most retailers hold – the customer’s payment card number. If retailers are not good custodians of payment data related to customers, they will no longer continue to frequent our establishments and use their credit and debit cards in our stores. When we examine the cybersecurity threats to all businesses, we should understand the basic underlying reason that retailers are being attacked is for payment card numbers in order to perpetrate card fraud.

We urge members of the Subcommittee to review and support legislative efforts designed to help mitigate the threat of cyberattacks as well as inform consumers of breaches of sensitive information *whenever* and *wherever* they occur. These issues are ones that we recommend you examine in a holistic fashion: we need to help prevent cyberattacks, and when attacks result in data breaches, help reduce fraud or other economic harm that may result from those breaches.

We should not be satisfied with simply determining what to do after a data breach occurs – that is, who to notify and how to assign liability. Instead, it is important to look at why such breaches occur, and what the perpetrators get out of them, so that we can find ways to reduce and prevent not only the breaches themselves, but the follow-on harm that is often the criminal motive behind these attacks. If breaches become less profitable to criminals, then they will dedicate fewer resources to committing them, and our data security goals will become more achievable.

With these guiding observations in mind, our statement below provides some initial comments on the Discussion Draft and the framework of proposed data security and breach notification legislation before this Subcommittee. We believe members of Congress and other Washington policymakers can work together to promote comprehensive breach legislation, which can be further bolstered by efforts within the private sector to improve data security practices outside of the lawmaking process. Retailers continue to invest in and promote technological security advancements, such as encryption and tokenization, that improve the security of our networks. We also believe there are ways to achieve greater security for the payment card itself since usable stolen card data is what drives the attacks on the retail industry networks. In our comments on proposed data breach legislation, we support several key elements that we believe would provide the best opportunity for Congress to establish a uniform, nationwide regime, based on the strong consensus of state laws, that applies to all businesses handling sensitive financial or personal information of consumers.

B. Where Breaches Happen Across Industry Sectors

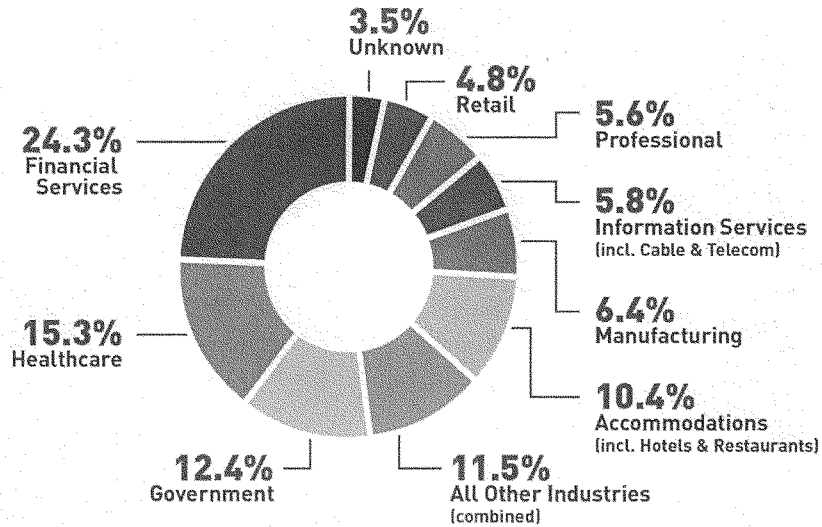
Unfortunately, cyberattacks and data breaches are a fact of life in the United States, and virtually every part of the U.S. economy and government is being attacked in some way. In its recently released *2017 Data Breach Investigations Report*,¹ Verizon examined 42,068 security incidents and 1,935 breaches, which it defines as security incidents resulting in “confirmed disclosure – not just potential exposure – of data to an authorized party.”² It found that the financial services sector accounted for the most breaches of all industry sectors, with nearly a quarter (24.3%) of all breaches occurring in the sector in the past year. Specifically, the Verizon report examined 998 security incidents in the financial services sector, concluding that 471 of them constituted data breaches due to confirmed disclosure of data to an unauthorized party.

In its tenth year, Verizon calls its report “the most authoritative, data-driven cybersecurity report” because it “leverages the collective data from 65 organizations across the world.” The Verizon breach report has been relied upon by investigators and analysts for a decade because it examines where breaches *occur* – including breaches undisclosed to the public – and does not just list which businesses publicly *report* having suffered a data breach. The report’s coverage of undisclosed breaches as well as reported ones distinguishes it from other breach studies based on reported breaches – this distinction is important because some businesses, like retailers and restaurants, are *required* to report data breaches in 48 states and 4 federal jurisdictions, while others, like financial institutions, are not required by federal law or many state laws to do so.

¹ Verizon’s *2017 Data Breach Investigations Report* is available at: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/>

² *Id.*, at p. ii.

The pie chart below illustrates where breaches occur, and it was created using the data in the Verizon report and, except for the “All Other Industries” category, uses the industry sector labels assigned by the report authors:



Source: Verizon 2017 Data Breach Investigations Report

The fact that more than half of all breaches occurred in just three sectors should not be a surprising revelation to Subcommittee members or staff when one considers that businesses in the financial services and healthcare sectors, along with U.S. government agencies, all handle American’s most sensitive financial, health and identity information. The criminal hackers attacking the banks, healthcare providers and government agencies, as well as other types of businesses with similar sensitive information, know which data is most valuable to them and has the longest shelf life on the black market where the stolen data is sold to other criminals. Data thieves focus far more often on banks, which hold our most sensitive financial and personal information – including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.

As shown by the pie chart, businesses with less sensitive data generally account for fewer breaches because the data is less valuable to thieves. For instance, according to Verizon’s report, the retail industry suffered just 4.8% of all breaches last year. Criminals are after the most valuable information they can find, and payment card numbers – which are immediately cancelled and replaced with new numbers when fraud is discovered – are not as valuable as bank account information that can lead to account takeovers and/or identity theft. It should also be noted that even these percentage figures above obscure the fact that there are far more merchants

that are potential targets of criminals in this area, as there are hundreds of times more merchants accepting card payments in the United States than there are financial institutions issuing cards and processing those payments.

Media reporting about data breaches is often disproportionate to the respective amount of security breaches in the banking and retail industry because, between them, only the retailers have strict, mandatory breach notification rules under all 48 state laws and 4 federal jurisdictions, including the District of Columbia, which require them to report data breaches whenever they occur. That is why consumers often hear far more about retail breaches in the news even though financial institutions have more than five times the number of breaches annually.

The latest breach report data from Verizon confirms the findings in many of its past reports, in that it reflects that significantly more data breaches occur at financial institutions than at retailers. What should be concerning to members of Congress and the public is that we rarely hear about any of the nearly five hundred security breaches in the financial services sector each year because banks, credit unions, and other financial institutions are not required to disclose them under federal banking law. The Equifax breach disclosure was the exception, not the rule.

Regardless of industry sector, there are far too many attacks that result in data breaches, and the breaches are often difficult to detect and are carried out in many cases by criminals with the latest technological methods at their disposal and significant resources behind them. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality. It is also a key reason why our proposed solutions include a call to harden the payment card system and protections against card fraud. Without fraud-prone payment card information in a retailer's system, criminals would find the rest of the information retailers hold – benign data such as phone book information, shoe size, color preference, etc. – to be fairly uninteresting and, more importantly, relatively worthless on the black market.

C. Achievable Solutions to Improving Cybersecurity

As noted above, protecting their businesses and customers from cyberattacks is of paramount importance to retailers. In today's world of networked systems, the retail industry also recognizes that it is going to take the highest level of collaboration and coordination to make sure we do it right. That means government, industry and law enforcement alike must work together to address and defend against the attacks facing American businesses.

Retailers are committed to safeguarding consumer data and working with the federal agencies and Congress to achieve practical solutions to these serious problems. Over the past several years, we have outlined a specific set of achievable solutions that we – and every industry with a stake in the issue – must work toward to better protect American consumers, empower our businesses and effectively safeguard America's cyberspace against criminal hackers. Specifically, we have urged policymakers to work toward these solutions:

- Support the passage of FEDERAL FRAUD PROTECTION FOR DEBIT CARDS, similar to what consumers enjoy for credit cards. Americans should not have to pay more for fraud protection.

- Call on the payment card industry to stop relying on fraud-prone signatures and issue PIN AND CHIP CARDS for all Americans, among the least protected cardholders in the world.
- Encourage all entities in the payments system — not just retailers — to ADOPT END-TO-END ENCRYPTION to protect consumers' payment information throughout the entire payments chain.
- Endorse the development of OPEN, COMPETITIVE TOKENIZATION STANDARDS to replace consumers' sensitive personal data (including payment card data) with non-sensitive "tokens" so that stored information is useless to would-be hackers.
- Continue support for a SINGLE NATIONAL DATA BREACH NOTIFICATION LAW that would establish a clear disclosure standard for all businesses to inform consumers of breaches whenever and wherever they occur.
- Support the passage of federal law enforcement legislation that would AID IN THE INVESTIGATION AND PROSECURITON OF CRIMINALS that breach our businesses' networks and harm our consumers.

In reviewing these proposals, we ask that you consider our views in each of these six areas of achievable solutions:

1. Federal Fraud Protection for Debit Cards

From many consumers' perspective, the credit and debit cards in their wallets are all simply payment cards. Consumers would be surprised to learn that their legal rights, when using a debit card – i.e., their own money – are significantly less than when using other forms of payment, such as a credit card. It would be appropriate if policy makers took steps to ensure that consumers' reasonable expectations were fulfilled, and they received at least the same level of legal protection when using their debit cards as they do when paying with credit.

NRF supports legislation that would immediately provide liability protection for consumers from debit card fraud to the same extent that they are currently protected from credit card fraud. This is a long overdue correction in the law and one concrete step Congress could take immediately to protect consumers that use debit cards for payment transactions.

2. Payment Card Security – "PIN and Chip" Cards

There are many technologies available that could reduce fraud resulting from payment card breaches, and an overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. Simply using the best network security technology available does not guarantee that a business can avoid suffering a security breach which exposes sensitive data, such as payment card numbers. Therefore, raising security standards alone may not be the most efficient or effective means of preventing potential harm to consumers from card fraud. With respect to payment card numbers, for example, it is possible that no matter how much security is applied by

a business storing these numbers, the numbers may be stolen from a business's database in a highly sophisticated security breach that can evade even state-of-the-art system security measures. Because of these risks, it makes sense for industry to do more than just apply increased network or database security measures.

One method to help prevent downstream fraud from stolen card numbers is to require more data or additional numbers from a consumer (such as their entry of a 4-digit personal identification number, or "PIN") to complete a payment transaction rather than simply permit the transaction to be approved based on the numbers that appear on the face of a card. Requiring this type of out-of-wallet information to authorize and complete payment card transactions is time-tested by the banking industry, as they have required the use of PINs to access bank accounts through ATM machines for decades. Use of PINs has been a minor inconvenience that American consumers have borne for the trade-off in increased security when accessing cash. Around the globe, the most industrialized nations – the G-20 – have also adopted PIN-based solutions for card transactions to replace the antiquated signature authentication methods that derive from the mid-twentieth century.

NRF believes it is time to phase out signature-authentication for all U.S.-issued payment cards – today's magnetic stripe cards as well as tomorrow's chip-based cards – and adopt a more secure authentication method for credit and debit card transactions. PINs can provide an extra layer of security against downstream fraud even if the card numbers (which the card companies already emboss on the outside of a card) are stolen in a breach. In PIN-based transactions, for example, the stored 20-digits from the card would, alone, be insufficient to conduct a fraudulent transaction in a store without the 4-digit PIN known to the consumer and not present on the card itself. These business practice improvements are easier and quicker to implement than any new federal data security law, and they hold the promise of being more effective at preventing the kind of financial harm that could impact consumers as companies suffer data security breaches affecting payment cards in the future.

In support of these concepts, on October 17, 2014, President Obama signed an executive order initiating the BuySecure Initiative for government payment cards.³ The order provided, among other things, that payment cards issued to government employees would include PIN and chip technology and that government equipment to handle and process transactions would be upgraded to allow acceptance of PIN and chip. Requiring PINs for all payment card transactions, as are required for some debit and ATM transactions (and some in-bank teller transactions as well) are common-sense actions that the banking industry should adopt immediately. Retail customers – American consumers – would be better protected by the replacement of a signature – a relic of the past – with the tried-and-true PIN that all other G-20 nations, including Canada, the U.K. and our European allies have adopted as part of their card payment system to protect their citizens.

As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This approach to payment card security should be adopted not only in the brick-and-mortar

³ 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>

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, like methods being developed in Canada and Europe. Adopting PIN-like protections for online purchases may help directly with the high percentage of U.S. fraud which occurs online.

3. Network Security – “End-to-End Encryption”

Encryption of payment card transaction data is another technological solution retailers employ to help defend against cyberattacks and that could help deter and prevent data breaches and the resulting fraud that can occur. Merchants are already required by Payment Card Industry (PCI) data security standards to encrypt cardholder data while being stored but, as not everyone in the entire payments chain is able to accept data in encrypted form during payment authorization, sensitive data may be left exposed (after it leaves the retailer’s system in encrypted form) at a critical time in the payment process. Payment security experts have therefore called for a change to require “end-to-end” (or “E2E”) encryption, which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the payment card data in encrypted form. This would require, as the PCI standards currently require of merchants but not of others in the payment stream, that card-issuing banks, merchant banks, branded payment card networks and payment card processors all adopt the same technology to handle encrypted payment card data. In fact, knowing that card chip technology alone is not the panacea touted by branded payment card networks, many retailers are not waiting for an E2E standard, and are investing, at significant costs, in point-to-point (or “P2P”) encryption.

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 in order to make use of it. We ask policymakers to urge our partners in the payments system, like we have, to adopt the most secure technologies to protect American consumers from card fraud. In the meantime, until all the stakeholders in the payments system adopt technology to enable “end-to-end” encryption, using PIN-authentication of payment cards now would offer some additional protection against fraud should the decrypted payment data today be intercepted by a criminal during its transmission “in the clear.”

4. Open, Competitive Tokenization Standards

Another sensible and achievable proposal to deter and protect against the harm that may result from cyberattacks is to minimize the storage and use by businesses of the full set of unredacted and unencrypted payment card numbers necessary to complete a transaction – a data protection principle known as “data minimization.” For example, a decade ago, the National Retail Federation asked the branded card networks and banks to lift the requirement that retailers store full payment card numbers for all transactions.

Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the “token”). Sensitive payment card data can be replaced, for example, with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been

available in the payment card space since at least 2005.⁴ Still, like the other proposed technological solutions above, tokenization is not a silver bullet solution, and it is important that whichever form of tokenization is adopted be one based on an open standard. This would help prevent a small number of networks from obtaining a competitive advantage, by design, over other payment platforms through the promotion of proprietary tokenization standards only.

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers would not need to have a physical payment card – and the mobile payments technology certainly would not need to replicate the security problem of physical cards that emboss account numbers on their face. It should also be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords, and increasingly, biometric finger prints. Indeed, if we are looking to leapfrog the already aging and fraud-prone current technologies, mobile-driven payments may be the answer.

As much improved as they are, the EMV chips rolled out on U.S. payment cards are essentially dumb computers. Their dynamism makes them significantly more advanced than the magnetic stripes still present on most Americans' payment cards, but their sophistication pales in comparison with the sophistication of even the most common smartphone. Smartphones contain computing power that could easily enable state-of-the-art fraud protection technologies. Smart phones are nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

5. National Data Breach Law

Each year the media is replete with news stories about data security breaches that raise concerns for all American consumers and for the businesses with which they frequently interact. Criminals focus on government agencies and U.S. businesses, including merchants, banks, telecom providers, cloud services providers, technology companies, and others. These criminals devoted substantial resources and expertise to breaching the most advanced data protection systems. Vigilance against these threats is necessary, but we need to focus on the underlying causes of breaches as much as we do on the effects of them.

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

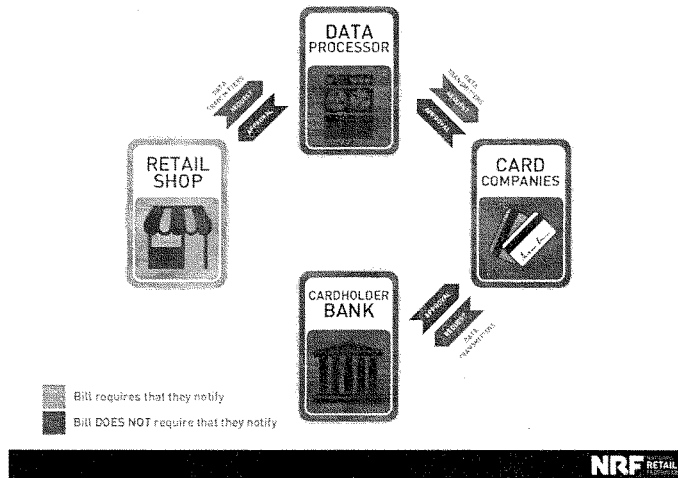
⁴ For information on Shift4's 2005 launch of tokenization in the payment card space see <http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lets-merchants-re-use-credit>.

across communications lines – for transmission or processing – or is stored in a “cloud,” it would be senseless for legislation to exempt these service providers, if breached, from comparable data security and notification obligations that the law would place upon any other entity that suffers a breach. Likewise, data breach legislation should not subject businesses handling the same sensitive customer data to different sets of rules with different penalty regimes, as such a regulatory scheme could lead to inconsistent public notice and enforcement.

Given the breadth of these attacks, if Americans are to be adequately protected and informed, federal legislation must cover all 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. Indeed, Congress could establish the same data breach notice obligations for *all* entities handling sensitive data that suffer a breach of security. Congress should not permit “notice holes” – the situation where certain entities are exempt from reporting known breaches of their own systems. If we want meaningful incentives to increase security, everyone needs to have skin in the game.

The chart below, however, illustrates how some legislative proposals like the Discussion Draft would operate with respect to notice by financial institutions or a “third party” operating in the payment system. This graphic shows a typical payment card transaction in which a card is swiped at a card-accepting business, like a retail shop, the information is transmitted via communications carriers to a payment processor, which in turn processes and transmits the data to a branded card network, such as Visa or MasterCard, which in turn processes it and transmits it to the card-issuing bank. (Typically, there also is an acquirer bank adjacent to the processor in the system, which the chart omits to provide greater clarity of the general payment flows.)

Consumers need to know when financial data is breached.



As currently drafted, the Discussion Draft would only require the retail shop, in this example above, to provide consumer notice of a breach of security. The payment processor, transmitter of the payment data (e.g., telecommunications carrier), or card company suffering a breach would qualify as a third party under the bill 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. The card-issuing bank suffering a breach would be exempt from the notification obligations to consumers or the public under the Discussion Draft.

Compared to the figures in Verizon’s 2017 Data Breach Investigations Report noted above, 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 payment system that suffers a breach, then 100% of the notices would come from the entities that suffer less than 5% of the breaches.

Breach Notification Exemptions for Financial Institutions

Many legislative proposals this Congress have “notice holes,” where consumers would not receive disclosures of breaches by certain entities. Perhaps the notice hole that has been left unplugged in most proposals, including the Discussion Draft, is the exemption from notification standards for entities subject to the Gramm Leach Bliley Act (GLBA), which itself does not contain any statutory language that requires banks to provide notice of their security breaches to affected consumers or the public.

Interpretive information security guidelines issued by federal banking regulators in 2005 did not address this lack of a requirement when it set forth an essentially precatory standard for providing consumer notice in the event banks or credit unions were breached. Rather, the 2005 interagency guidelines state that banks and credit unions “should” conduct an investigation to determine whether consumers are at risk due to the breach and, if they determine there is such a risk, they “should” provide consumer notification of the breach.⁵ These guidelines fall short of creating a notification *requirement* using mandatory language like “must” – an imperative command that could be used legislation to require breach notification for financial institutions. Instead, banks and credit unions are left to make their own determinations about when and whether to inform consumers of a data breach. **(In Appendix A, we have provided a two-page analysis of the use of “should” and other precatory language in the security guidelines that demonstrates there is no mandatory data breach notification requirement for financial institutions under GLBA or its interpretive guidance.)**

Several accounts 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 in 2014 that as many as one dozen financial institutions were targeted as part of the same cyberattack scheme.⁶

⁵ 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>

⁶ “JP Morgan Hackers Said to Probe 13 Financial Firms,” *Bloomberg* (Oct. 9, 2014).

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 the affected institutions been made public. The lack of transparency and dearth of information regarding these incidents reflects the fact that banks are not subject to the same requirements to notify affected customers of their own breaches of security as other businesses are required now under 48 state laws. A few of the more seasoned and robust state laws, such as California's breach notification law, have not exempted financial institutions from their state's breach notification law because they recognize that banks are not subject to any federal requirement that says requires them to notify customers in the event of a breach of security.

General Principle: The Breached Entity Should Have Notification Obligations

With respect to establishing a national standard for breach notification, the only principle that makes sense is that breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of sensitive information on their systems. Just as the Federal Trade Commission (FTC) expects there to be reasonable data security standards employed by each business that handles sensitive personal information, a federal breach notification bill should apply notification standards that "follow the data" and apply to any entity in a networked system that suffers a breach of security when sensitive data is in its custody.

Some have called upon entities that are "closest to the consumer" to provide breach notice in all cases for any third party that handles data for that entity. As shown in the example above, however, we would suggest that the one-to-many relationships that exist in the payment card system and elsewhere will ultimately require potentially thousands of businesses to all notify about the same breach – another business's breach. This is not the type of transparent disclosure policy that Congress has typically sought.

An effort to promote relevant notices should not obscure transparency as to where a breakdown in the system has occurred. Indeed, a public notice obligation on all entities handling sensitive data would create significant incentives for every business that operates in our networked economy to invest in reasonable data security to protect the sensitive data in its custody. By contrast, a federal law that permits "notice holes" in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public's trust.

Data Security Standards

Data security standards vary depending on the nature of an entity's business and where it operates. Over the past half-century, the United States has essentially taken a sector-specific approach to data privacy requirements (including data security measures), and our current legal framework reflects this. For example, credit reporting agencies, financial institutions, and health care providers, just to name a few regulated sectors, have specific data security standards that flow from laws enacted by Congress, such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), respectively.

The agencies that have implemented section 501(b) of GLBA—the Federal Financial Institutions Examination Council (FFIEC), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (Fed Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS)—have defined a process-based approach to security in the *Interagency Guidelines Establishing Information Security Standards* (“Security Guidelines”)⁷ Under the Security Guidelines, however, when designing security controls a financial institution is required to design an information security plan that “controls the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope” of the entity’s activities and, in so doing, must consider certain security measures and only if appropriate, adopt them.⁸ Significantly, one of these security measures that a financial institution must consider, but is not required to adopt, is a “response program that specify actions to be taken when the institution suspects or detects that *unauthorized individuals have gained access to customer information systems*, including appropriate reports to regulatory and law enforcement agencies.”⁹ (*emphasis added*)

Those operating in other industry sectors that are subject to the jurisdiction of the Federal Trade Commission (FTC) must abide by the standards of care enforced by the FTC under Section 5 of the FTC Act, which give the Commission broad, discretionary authority to prosecute “unfair or deceptive acts or practices” (often referred to as their “UDAP” authority). On top of this federal statutory and regulatory framework, states have regulated businesses’ data security practices across a variety of industry sectors and enforced consumer protection laws through their state consumer protection agencies and/or their attorneys general.

Legal exposure for data security failures is dependent on the federal or state laws to which a business may be subject and is alleged to violate. The FTC, for example, has been very active in bringing over 50 actions against a range of companies nationwide that are not otherwise subject to a sector-specific federal data security law (e.g., GLBA, HIPAA, etc.). For example, under its Section 5 UDAP authority, the FTC has brought enforcement actions against entities that the Commission believes fall short in providing “reasonable” data security for personal information. Nearly all of these companies have settled with the FTC, paid fines for their alleged violations (sometimes to the extent of millions of dollars), and agreed to raise their security standards and undergo extensive audits of their practices over the next several decades to ensure that their data security standards are in line with the FTC’s order.

Effect of Imposing GLBA Guidelines for Financial Institutions as Mandatory Requirements on Commercial Businesses Subject to FTC Enforcement

NRF supports federal data security standards for all entities handling sensitive consumer information, but federal standards to be enforced by the FTC against the wide range of businesses under its jurisdiction would fall under the Commission’s broad and discretionary authority to prohibit “unfair or deceptive acts or practices” and should be enforced consistent with the Commission’s long-standing practices under Section 5 of the FTC Act.

⁷ Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS).

⁸ *Id.* at ¶ III, C.1.

⁹ *Id.* at ¶ III, C.1.g.

The FTC standard is consistent with the consumer protection standard that applies to financial institutions. Under Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the Consumer Financial Protection Bureau (CFPB) was established and granted the authority to prohibit “unfair, deceptive or abusive acts or practices” for consumer financial products and services.¹⁰ As the CFPB explains in the CFPB Supervision and Examination Manual, “Unfair, deceptive, or abusive acts and practices (UDAAPs) can cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace.”¹¹ NRF is not aware of any financial institutions that have suggested that the CFPB standard is too weak.

Providing the FTC with different authority – to enforce process-based data security standards like those in the Security Guidelines implementing GLBA, as proposed in the Discussion Draft – would be an unprecedented and dramatic expansion of the FTC’s authority that is unjustified in its application to the broad array of businesses subject to its jurisdiction. The Security Guidelines were designed for banking regulators that take an audit/examination approach to regulating companies and work with them through an iterative process to help the institution come into compliance where it may be lacking, without the threat of severe penalties. The FTC, by contrast, takes an enforcement approach, which under a GLBA-like guidelines standard, would require a post-hoc determination of a company’s compliance with an amorphous standard in a world where the technological threat vectors are ever-changing.

In an adversarial investigatory process, like the kind the FTC employs in its enforcement of Section 5 of the FTC Act, entities are either guilty or not, and more likely to be guilty by the mere fact of a breach. Unlike financial institutions subject to the Security Guidelines, companies subject to FTC enforcement of its UDAP authority are not able to get several bites at the apple working with regulators until they know they are in compliance with the regulator’s vision of data security. Rather, businesses facing FTC enforcement would have to guess at what will satisfy the agency and, if their security is breached, the strong enforcement presumption would be that the company failed to meet the subjective standard.

Because of this disparity in how security guidelines would be enforced, NRF sought an expert opinion on the effect of federal legislation that would impose banking industry-based data security standards on a vast array of commercial businesses, ranging from large nationwide companies to small, single-location businesses that are not “financial institutions.” This would include every non-banking business in America that accepts virtually any form of tender other than cash (e.g., credit cards, debit cards, checks, etc.) in exchange for goods and services. **As part of your efforts to examine this issue, we strongly encourage you to review the white paper – attached as *Appendix B* to this testimony – that was prepared by two former associate directors responsible for financial and credit practices in the FTC’s Bureau of Consumer Protection.** The authors’ 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 business in the U.S. economy would be a

¹⁰ The text of the Act is available at: <http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf>

¹¹ CFPB Supervision and Examination Manual, Version 2, October 2012, p. 174 (UDAAP 1), available at: http://www.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf

dramatic expansion of regulatory authority that is unprecedented in its scope and unjustified in its application.

Finally, the different enforcement regimes between financial institutions and entities subject to the FTC's jurisdiction is also evident in the manner and frequency with which fines are assessed and civil penalties imposed for non-compliance with a purported data security standard. Banks are rarely (if ever) fined by their regulators for data security weaknesses. But, as noted above, commercial companies have been fined repeatedly by the FTC. Providing an agency like the FTC, with an enforcement approach, a set of standards with significant room for interpretation is likely to lead to punitive actions that are different in kind and effect on entities within the FTC's jurisdiction than the way the standards would be utilized by banking regulators in an examination. A punitive approach to companies already victimized by a crime would not be appropriate nor constructive considering that the FTC itself has testified before Congress that no system – even the most protected one money can buy – is ever 100% secure.

Preemption – Establishing a Nationwide, Uniform Standard of Notification

For more than a decade, the U.S. federalist system has enabled every state to develop its own set of disclosure standards for companies suffering a breach of data security and, to date, 48 states and 4 other federal jurisdictions (including the District of Columbia and Puerto Rico) have enacted varying data breach notification laws. Many of the states have somewhat similar elements in their breach disclosure laws, including definitions of covered entities and covered data, notification triggers, timeliness of notification, provisions specifying the manner and method of notification, and enforcement by state attorneys general. But they do not all include the same requirements, as some cover distinctly different types of data sets, some require that certain state officials be notified, and a few have time constraints (although the majority of state laws only require notice “without unreasonable delay” or a similar phrase.)

Over the past ten years, businesses such as retailers, to whom all the state and federal territory disclosure laws have applied, have met the burden of providing notice, even when they did not initially have sufficient information to notify affected individuals, through standardized substitute notification procedures in each state law. However, with an increasingly unwieldy and conflicting patchwork of disclosure laws covering more than 50 U.S. jurisdictions, it is time for Congress to acknowledge that the experimentation in legislation that exists at the state level and that defines our federalist system has reached its breaking point, and it is time for Congress to step in to create a national, uniform standard for data moving in interstate commerce in order to ensure uniformity of a federal act's standards and consistency of their application across jurisdictions.

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

In sum, passing a federal breach notification law is a common-sense step that Congress should take now to ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.

Preemption of state laws and common laws that create differing disclosure standards is never easy, and there is a long history of Supreme Court and other federal courts ruling that, even when Congress expresses an intent to preempt state laws, limiting the scope of the preemption will not result in preemption. All it will accomplish is to add yet another law, this time federal, to the state statutes and common laws already in effect, resulting in the continuation of a confusing tapestry of state law requirements and enforcement regimes. A federal act that leaves this in place would undermine the very purpose and effectiveness of the federal legislation in the first place.

In order to establish a uniform standard, preemptive federal legislation is necessary. But that does not mean (as some have contended) that the federal standard must or should be “weaker” than the state laws it would replace. On the contrary, in return for preemption, the federal law should reflect a strong consensus of the many state laws. Some have called for a more robust notification standard at the federal level than exists at the state level. Without adding unnecessary bells and whistles, NRF believes that Congress can create a stronger breach notification law by removing the exemptions and closing the types of “notice holes” that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses. This approach would enable members that are concerned about preempting state laws to do so with confidence that they have created a more transparent and better notification regime for consumers and businesses alike. It is a way this Congress can work to enact a law with both robust protection and preemption.

We urge Congress, therefore, in pursuing enactment of federal breach notification legislation, to adopt a framework that applies to all entities handling sensitive personal information 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.

6. Greater Investigation and Prosecution of Cyber Criminals

In addition to the marketplace and technological solutions suggested above, NRF would also support a range of legislative solutions that we believe would help improve the security of our networked systems and ensure better law enforcement tools to address criminal intrusions.

Most important among these legislative solutions would be efforts to strengthen our extra-territorial law enforcement. As noted in our introduction above, industry sectors across the U.S. share the collective concern and face the same threat to their businesses’ networks that appear to come predominantly from foreign actors. If the U.S. economy were threatened by foreign actors that had the most sophisticated technology to counterfeit our U.S. dollars, and were using it to perpetrate fraud in the United States and disrupt our economy, would Congress only be asking the victimized companies that unknowingly accepted counterfeit cash as payment why they did not better protect their customers from this fraud? We think that Congress, in this

hypothetical, would look first toward the criminal actors and enterprises that were perpetrating these crimes on our shores.

We therefore call upon Congress to develop legislation that would provide more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches – particularly those with foreign attack signatures – are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

C. Conclusion

Like financial institutions, American retailers are targets of cybercrime but suffer less than 5% of all security breaches. They do so predominantly because of the payment card data they accept and process. Criminals desire U.S.-based card numbers because they are unprotected and easily sold on the global black market to would-be fraudsters. The data thieves and their criminal customers – the purchasers of these stolen card numbers – realize the short lifespan of stolen card numbers once a breach is detected. That is why the criminals that hack American businesses typically go to extraordinary lengths to mask their incursions with methods that have not been seen before and that are not addressed by network security solutions. In short, if they can act undetected in this “cat-and-mouse” game, and place stolen card numbers on the black market before law enforcement and victimized businesses know the cards are there, they can drive up the market price for the stolen cards.

As stated earlier, retailers have invested billions in adopting data security technology. Efforts to promote payment card security, end-to-end encryption and tokenization are highlighted in the discussion above. The dominant card networks and card-issuing banks, however, have not made all the technological improvements suggested above that would make the payment cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe. Our ability to improve payment card security and protect American consumers in the chain of the American payment ecosystem is, and will only be, as strong as its weakest link. Without the cooperation of our partners in the financial system, we cannot alone affect the changes necessary to better defend and protect against cyberattacks that lead to payment card fraud. Everyone already has skin in the game, and we need to work together to do what we can to improve an aging and outdated payment system that is the principal target of cyberattacks affecting U.S. retail businesses and their customers.

While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft that result from cyberattacks, there is much left for card-issuing banks and payment card networks to contribute, as retailers are doing, to better protect our payment system and the fraud-prone cards that are used in them. That is why we have proposed practical, commonsense and achievable solutions above that NRF believes are necessary to helping deter and defend against cyberattacks affecting the retail industry. We appreciate the opportunity to submit this statement to the Subcommittee today, and we look forward to working with the members of the Subcommittee and full Committee on Financial Services to bring greater attention to these issues and help push forward some or all of our proposed solutions to improve cybersecurity in across all industry sectors.

Appendix A:

Financial Institutions'
Data Breach Notification Provisions under the
Gramm-Leach-Bliley Act

Data Breach Notification Provisions and the Gramm-Leach-Bliley Act

Financial institutions are not required under federal law to notify customers of data breaches. While some have pointed to the Gramm-Leach-Bliley Act (“GLBA”) as the source of such a requirement, the GLBA does not require notification of consumers of data breaches. The GLBA instructs the Office of the Comptroller of the Currency (“OCC”), the Federal Reserve Board (“Board”), the Federal Deposit Insurance Corporation (“FDIC”), and the Office of Thrift Supervision (“OTS”) to establish “security and confidentiality” standards for financial institutions. Those agencies have developed guidelines, not regulations, to implement that part of GLBA.¹

The bottom line is that there is no data breach notification provision or requirement under the Gramm-Leach-Bliley Act.² The guidelines established by the above agencies do not speak in mandatory terms. Instead they provide:

- When designing security controls, financial institutions need to “consider” a data breach response plan but are not required to develop a data breach response program or notify consumers after a breach.³
- According to the Incident Response Guide, financial institutions “should” have a data breach response program, but they are not required to have one.⁴
- “At a minimum, an institution’s response program should contain procedures for...Notifying customers when warranted.”⁵ When notification is “warranted” is left to the discretion of the financial institution.
- “The proposed Guidance stated that an institution should notify affected customers whenever it becomes aware of unauthorized access to “sensitive customer information” unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur . . .”⁶
- “The guidance is an interpretation of existing provisions in section 501(b) of the GLBA and Information Security Guidelines. Therefore, a delayed effective date is not required. Financial institutions should implement the interpretive guidance as soon as possible.

¹ *Interagency Guidelines Establishing Information Security Standards*, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS) [hereinafter *Security Guidelines*]; *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) [hereinafter *Incident Response Guidance*].

² Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827).

³ *Security Guidelines*, *supra* note 3, at ¶ III, C.1.g.

⁴ *Incident Response Guidance*, *supra* note 4, at ¶ II, A.

⁵ *Incident Response Guidance*, 70 Fed. Reg. at 15740.

⁶ *Incident Response Guidance*, 70 Fed. Reg. at 15743.

The agencies recognize that not every financial institution currently has a response program that is consistent with the interpretive guidance. The agencies will take into account the good faith efforts made by each institution to develop a response program that is consistent with the interpretive guidance, however; any financial institution experiencing a breach in security that includes unauthorized access to customer information is expected to respond promptly in a manner consistent with the guidance, and provide customer notice, if warranted.⁷

- “The final Guidance provides that when an institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused.”⁸
- “If the institution determines that misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible.”⁹ So, even if a financial institution knows that stolen information has been misused, it is still not required to notify customers.

⁷ Financial Institution Letter FIL-27-2005 (April 1, 2005) available at <https://www.fdic.gov/news/news/financial/2005/fil2705.html>.

⁸ *Incident Response Guidance*, 70 Fed. Reg. at 15743.

⁹ *Incident Response Guidance*, 70 Fed. Reg. at 15743.

Appendix B:

White Paper on Application of
Safeguard Requirements for Banks to
Nonfinancial Institutions

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 Chr 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).



STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE
BUREAU OF INTERNET
AND TECHNOLOGY

March 7, 2018

VIA EXPRESS MAIL

The Honorable Jeb Hensarling
Chairman
Committee on Financial Services
U.S. House of Representatives
2228 Rayburn House Office Building
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
U.S. House of Representatives
2221 Rayburn House Office Building
Washington, DC 20515

The Honorable Blaine Loutkemeyer
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
U.S. House of Representatives
2230 Rayburn House Office Building
Washington, DC 20515

The Honorable Wm. Lacy Clay
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
U.S. House of Representatives
2428 Rayburn House Office Building
Washington, D.C. 20515

Re: Data Acquisition and Technology Accountability and Security Act

Dear Chairman Hensarling, Ranking Member Waters, Chairman Loutkemeyer, and Ranking Member Clay:

I write to address recently proposed legislation entitled the Data Acquisition and Technology Accountability and Security Act, a discussion draft released on February 16, 2018, which seeks to establish federal standards for data security and data breach notification.

I was pleased to testify before the Committee on Financial Services on October 25, 2017,¹ during a continuation of the Committee's prior hearing on the Equifax data breach. I 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.

¹ I recently submitted similar written testimony to the Senate Committee on Commerce, Science, and Transportation in connection with that Committee's February 6, 2018 hearing on the recent Uber breach.

Nonetheless, I write in connection with the Committee’s hearing on March 7, 2018 to express concerns about the bill as currently drafted. In particular, the bill would unwisely retract existing protections for consumers at a time when such protections are essential. These concerns are informed by the New York State Attorney General’s (“NYAG”) experience enforcing New York’s data security laws, including its notification law (General Business Law § 899-aa) and social security safeguards law (General Business Law § 399-ddd), and our strong record of cooperating with other State Attorneys General in investigations of major breaches.

I. The Bill Should Not Preempt State Law and the Preemption is Too Broad.

As a threshold matter, our office and many states are concerned about any law that preempts state data breach law, as many states have breach notification laws that are more protective of consumers than some notification language considered in most proposed federal legislation. In 2005, the NYAG joined a bi-partisan coalition of forty-three State Attorneys General in a letter to Congress calling for a national law on breach notification that did not preempt state enforcement or state law.² The letter stated:

Do not preempt the power of states to enact and enforce state security breach notification. . . . Preemption interferes with state legislatures’ democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government.

State AGs repeated that bi-partisan plea with forty-six other State Attorneys General to Congressional Leaders on July 7, 2015.³ Any bill should not preempt state law. It should merely set a floor for data security and notification protocols in the event of a breach. States must continue to be able to innovate in the areas of data security and breach notification and have authority to pass laws that exceed the federal standard to keep pace with technological advances and protect consumers.

Not only does the current draft of the bill preempt state law, but it does so in a way that is vague and could be broadly interpreted. The bill would preempt any state laws “with respect to securing information from unauthorized access or acquisition, including notification of unauthorized access or acquisition of data. . . .” A variety of state laws could be said to be “with respect to securing information from unauthorized access or acquisition.” For example, a state law criminalizing hacking of data, or accessing data in an unauthorized way, or data theft (or even receipt of stolen data) could be said to come within the ambit of this language. Indeed, this language could even be read to preempt anti-stalking laws as applicable to stalking online, or a law requiring the data held at particularly sensitive locations (such as a domestic-violence shelter) be stored securely. States would also have difficulty crafting consumer privacy legislation, such as limiting a company’s ability to collect or sell the personal information of consumers or requiring companies to delete information upon request or after closing an account.

² Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (Oct. 27, 2005).

³ Letter to Congressional Leaders from NAAG (July 7, 2015).

Indeed, this broad language could be read to prohibit a state from passing *any* law covering any aspect of data security or privacy.

The problem stems, in part, from the preemption clause's reference to the undefined word "information," while the data security and breach notification provisions of the bill only apply to "personal information," as narrowly defined. There is a wide gap between what constitutes "information" and the narrow set of "personal information" the bill covers. That means a broad spectrum of laws concerning types of information not protected by the bill may be left at risk were the bill to become law in its current form.

II. Harm-Based Notice Misconstrues the Purpose of Notification and Is Too Limiting.

The bill's notification obligation is only triggered if the breached company determines that there is "reasonable risk that the breach of data security has resulted in or will result in identity theft, fraud, or economic loss to the consumers to whom the personal information involved in the incident relates..." This is a mistake for a variety of reasons.

First, the bill triggers the notice obligation based only on the determination by the potentially-breached entity. There is no requirement that this determination be supported, nor does the bill provide guidance as to how that determination is to be made. In our experience, companies may have self-serving reasons for keeping breaches secret or minimizing reports of harm. Indeed, it is very difficult to determine what specific harm may or may not occur following a breach. Consumers should be informed immediately so they (and not the company) can decide if they are at risk of harm and thus need to take steps to protect themselves.

Second, companies may interpret this requirement narrowly to avoid giving notice of a breach. For example, the NYAG recently investigated a credit card breach at Hilton Domestic Operating Company, Inc, which owns, manages, or franchises a portfolio of brands including Hilton Hotels & Resorts, Waldorf Astoria Hotels & Resorts, and DoubleTree by Hilton.⁴ Hilton found credit-card targeting malware on its payment systems, as well as "dump files" with tens of thousands of credit card numbers. Often, identity thieves will aggregate the credit-card numbers in "dump files" immediately prior to removing them from the computer system. However, Hilton did not provide notice to consumers or NYAG because—it argued—it did not find definitive evidence of removal of the credit card numbers from its computer environment. However, through its investigation, NYAG learned that Hilton lacked a complete set of log files that could have revealed the removal or exfiltration of the data. Additionally, the intruders used anti-forensic tools that could hide evidence of exfiltration of the credit card numbers. Ultimately, NYAG found that Hilton should have notified consumers of the incident so that the consumers could take the necessary steps to protect themselves.

In short, any rule that allows the breached company itself to determine whether there is "reasonable risk" of identity theft leaves too much discretion in the hands of a company that has financial and reputational motives not to provide notice.

⁴ <https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed>

Finally, even if there is no harm or likelihood of harm resulting from the breach, we believe that companies should still be required to provide notice to both consumers and regulatory agencies. These disclosures result in necessary public accountability that provides companies with extra motivation to adopt better data security. Notice also helps regulators and the public at large understand data breaches and breach trends, and to investigate the reasons for them. Since the adoption of the first state data breach notification law in 2003, the public's understanding of the extent of the threat posed by data breaches has matured, in large part thanks to the ubiquity of data breach notification laws.

For these reasons, consumers are best protected when the circumstances under which a company must provide notice are not as limited as provided in the bill.

III. The Bill Fails to Require Notice to NYAG To Ensure Meaningful Enforcement.

While the bill's apparent requirement of notice of a breach to the Federal Trade Commission ("FTC") is an important step for enforcement of the bill's requirements, it is not by itself enough. Where state law so provides, companies should also be required to provide notice to any State Attorney General office if the state's consumers are affected. Pursuant to GBL § 899-aa, the NYAG receives notice of over a thousand breaches a year if they affect a New York consumer. This notification allows us to investigate cases where a company (i) did not provide notice to consumers in a reasonable amount of time and (ii) failed to protect consumers' personal information with reasonable data security. Without such notification, State Attorneys General are left without any means to learn of a data breach affecting their citizens and, accordingly, will be stripped of any meaningful opportunity to enforce the bill's notification and data security requirements.

IV. The Bill's Notice Provision Misses the Majority of Data Breaches.

The bill only requires notice to the FTC and consumers if 5,000 or more consumers are affected. While the mega-breaches at companies like Equifax, Target, and Home Depot receive media attention, consumers deserve to be informed when their personal information has been compromised, for all breaches.

In 2017, the NYAG received 1,583 data breach notifications. 1,256 of the 1,583 involved a breach of less than 5,000 consumers nationwide, representing close to 80% of total breaches reported. If the 5,000-consumer threshold was the rule in New York in 2017, the NYAG would have received only 327 notices instead of 1,583. Without learning of the bottom 80% of breaches, the NYAG and other State Attorneys General offices cannot protect their citizens. And if consumers are not informed about breaches, they cannot protect themselves.

V. The Bill Infringes on the States' Consumer Protection Enforcement Authority.

While the bill gives the State Attorneys General the option of filing 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 proceeds in filing an action or otherwise intervenes. Such restrictive requirements infringe on the sovereign enforcement prerogatives of the NYAG and other State Attorneys General, inject unnecessary delay and costs, and complicate 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 New York's counterpart (General Business Law §§ 349 and 350), 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 sovereign enforcement prerogative of NYAG and the other states.

Moreover, the provision of the bill requiring consolidation of State Attorneys General actions into a single court sets a bad precedent and is unnecessary. The bill provides if two or more State Attorneys General file an action, then such proceedings *must* be consolidated in the District of Columbia. However, it makes little sense to say that if a breach by a west coast company uniquely impacts Californians and Oregonians that those States Attorneys General would have to proceed only in a federal court 3,000 miles away, so far from those States and their interested residents. Nor should either State's sovereign interests in protecting their own residents be *compelled* to join together as plaintiffs in a single case. To the extent there is any need to coordinate cases in the federal judiciary, there is a well-established multi-district litigation (“MDL”) procedure that facilitates pre-trial procedures and settlement.

VI. The Bill Should Not Carve Out Financial Institutions.

The bill's treatment of financial institutions is also problematic. Section 5 of the bill provides that if a financial institution maintains policies that are “designed to comply” with its existing obligations under Section 501(b) of the Gramm-Leach-Bliley Act then the institution is “deemed in compliance” with the security and breach notice requirements of the bill. Unfortunately, many businesses maintain policies that are “designed to comply” with legal requirements, and yet do not comply, and thus still violate the law.

Moreover, whereas today financial institutions are subject to joint enforcement efforts by their respective federal regulators and State Attorneys General in this area, the bill neuters States in this regard. It states: “An attorney general of a State may not file an action under this subsection against any covered entity that is a financial institution, or its affiliates.” So, as to financial institutions, the bill is a windfall because it *removes* State investigative and enforcement authority that they are subject to under current law, without providing States with enforcement authority even in the new federal regime.

Breaches are a growing problem, including in the financial sector, which hold consumers' most sensitive financial information. Credit reporting agency Equifax just reported one of the largest breaches ever, in which more than 8 million New Yorkers' social security numbers were stolen. The bill, if enacted, would preempt New York's investigation and any state enforcement

action against Equifax—not to mention the bill’s impact on state investigations and enforcement against in the aftermath of future, similar breaches. That is not good policy.

VII. The Preliminary Investigation Requirement Must Be Done Expeditiously.

The bill requires that an entity that has experienced a breach conduct a preliminary investigation prior to providing notice to consumers or regulators. Though the bill describes this as an “immediate investigation,” the bill does not require the investigation to be completed expeditiously or within any particular period of time. With no compulsion to do otherwise, companies often take months, and in some cases years, to complete such an investigation. This provision puts no impetus on companies to complete the investigation expeditiously—and thereby delays notifications to consumers, whose financial well-being may hang in the balance. The requirement to provide notice “without unreasonable delay” should include the required preliminary investigation.

VIII. Conclusion

The Committee is right to explore the topics of data security and breach notification, and I appreciate the opportunity to appear before the Committee last year and to comment on the Discussion Draft circulated in recent weeks. For the reasons stated above, the bill as currently drafted raises concerns, particularly in terms of its how it interacts with state law, law enforcement, and our bread-and-butter consumer protection work. As “laboratories of democracy,” the States first adopted a data breach notification requirement, and the States have continued to legislate to respond to technical innovation, including adding notification for online credentials and biometric identifiers. States have a strong track record of protecting consumers in this area. Congress should allow the states, and their law enforcement entities, to continue to play this traditional role.

Sincerely,



Kathleen McGee
Bureau Chief
Bureau of Internet and Technology

March 7, 2018

The Honorable Blaine Luetkemeyer, Chairman
 The Honorable William Lacy Clay, Ranking Member
 United States House of Representatives
 Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit

Thank you for the opportunity to provide feedback to the discussion draft of the "Data Acquisition and Technology Accountability and Security Act."¹ Below are several key improvements we wish to suggest for your consideration, focused largely on the draft's data security requirements, with the goals of strengthening cybersecurity and protecting organizations and consumers from data breaches.

I) Preemption: In general, we support a unified standard for private sector data security and breach notification to facilitate understanding and compliance of the law by a broad range of organizations. Section 6 of the discussion draft includes a preemption provision that would encompass both state and federal information security laws for both the private and public sectors.² However, if all current information security laws are preempted, the federal replacement should not establish substantially weaker protections than the status quo. We believe the legislation should be strengthened before setting a national standard.

- o **Recommendation 1:** Strengthen the bill's security safeguard requirements and definition of personal information. Alternatively, preempt only the covered information and security requirements as articulated in the bill, enabling states and federal agencies to provide additional protections outside these areas. Consider excluding government agencies' internal security requirements from preemption.

II) Personal information definition: The discussion draft, in Sec. 2(10)(A)(iv), defines "personal information" to include only usernames/passwords that are required for an individual to purchase goods or services. In addition, Sec. 2(10)(A) of the draft defines "personal information" as always requiring an individual's actual name. Under these definitions, no data security or breach notification requirements would apply to usernames/passwords for online accounts not necessary for transactions, such as accounts containing written correspondence, personal media (photos, gaming, etc.), medical information (not covered by HIPAA/HITECH), and more. In addition, no data security or breach notification requirements would apply to usernames/passwords or biometric authenticators unless the user's actual name were also included.

Modernized cybersecurity standards should reflect that credentials for online accounts should receive some level of protection against unauthorized access – even if the credentials are not required to complete purchases, or if the credentials do not include the user's actual name.

¹ Data Acquisition and Technology Accountability and Security Act, discussion draft, 115th Cong., <https://financialservices.house.gov/uploadedfiles/bills-115-datasa-pih.pdf> (last accessed Mar. 6, 2018).

² The "covered entity" definition in Sec. 2(7) includes persons, businesses, nonprofits, and government agencies.

Stolen and misused credentials are a major attack vector and source of breach, even without a user's name and in both financial and nonfinancial contexts.³ A breached username/password or biometric authenticator can yield a user's actual name, and credentials are often reused across accounts.⁴ Several states require the private sector to protect credentials for online accounts, without limiting protection to credentials necessary for purchases and/or accounts that include actual names.⁵

- **Recommendation 2:** Modify Sec. 10(A)(iv) to include protection for usernames in combination with passwords or access codes for online accounts, rather than just credentials required to make purchases.
- **Recommendation 3:** Separate username/password and biometric authenticators from the actual name requirement in Sec. 10(A).

III) Security safeguards requirement: Data security safeguards are critical to preventing breaches before they occur. Breach notification requirements and common law causes of action only apply after a breach has occurred. A national data security requirement should remain effective over time for a variety of organizations without undue burden. To this end, we support the flexibility of safeguards in Sec. (3)(a)(2), and the risk-based approach in Sec. 3(a)(3).

However, the draft bill's security safeguard requirement would potentially undermine cybersecurity. Under Sec. 3(a)(1), safeguards are limited to the protection of personal information from acquisition that is reasonably likely to result in identity theft, fraud, or economic loss. This draft security standard is considerably narrower than many current federal and state protections. For example, Executive Order 13800 requires federal agencies to use the NIST Cybersecurity Framework to manage cybersecurity risk, yet the Cybersecurity Framework is not restricted to protection against acquisition reasonably likely to result in economic harm.⁶ Numerous states require the private sector to safeguard personal information,⁷ and nearly half of all states require public agencies to safeguard their confidential

³ See Verizon Data Breach Investigations Report, 2017, pgs. 3-7, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017>. Approximately four out of five breaches involved stolen or weak credentials.

⁴ See Statement of Troy Hunt for the House Committee on Energy and Commerce, Identity Verification in a Post-Breach World, pgs. 9-11, Nov. 30, 2017, <http://docs.house.gov/meetings/IF/IF02/20171130/106662/HHRG-115-IF02-Wstate-HuntT-20171130.pdf>. Frequent redistribution and aggregation of breached data has made it easier to combine data elements from multiple breaches and open sources.

⁵ California Civ. Code 1798.81.5(d)(1). Florida Stat. 501.171(1)(g)(b). Maryland Code Com. Law 14-3501(e). Minnesota Stat. 325M.01. Nevada Rev. Stat. 603A.040 (protects non-purchase accounts but requires name).

⁶ Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017, Sec. 1(c)(ii), <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure>.

⁷ Arkansas Code Ann. 4-110-104. California Civ. Code 1798.81.5(b). Connecticut Gen. Stat. § 42-471(a). Florida Stat. 501.171(2). Indiana Code 24-4.9-3-3.5. Kansas Stat. 50-6.139b(b)(1). Massachusetts Gen. Laws Ch. 93H § 2(a). Minnesota Stat. 325M.05. New Mexico Stat. 57-12C-4. Nevada Rev. Stat. 603A.210. Oregon Rev. Stat. 646A.622(1). Rhode Island Gen. Laws 11-49.3-2. Texas Bus. & Com. Code 521.052. Utah Code 13-44-201.



information or systems,⁸ without limiting these safeguards to protection against risks of economic harm.

- **Recommendation 4:** Modify the security safeguard requirement in Sec. 3(a)(1) to protect against risks identified in the risk assessment required under Sec. 3(a)(3). Alternatively, in Sec. 3(a)(1), strike the phrase "that is reasonably likely to result in identity theft, fraud, or economic loss" and replace it with "access, or modification."

IV) Delay of breach notification: The discussion draft, in Sec. 4(b)(5), requires covered entities to delay notification of a breach to consumers when requested by federal or state law enforcement agencies. However, the bill does not establish any process, justification, or time limit to the delay of notification, which may unnecessarily restrain data owners from notifying affected parties of a potentially harmful breach.

- **Recommendation 5:** Clarify the circumstances under which a law enforcement agency may request delay of notification. For example, some states with similar provisions permit a request to delay when notification would jeopardize an investigation, and require the request to be made in writing with a specified delay period.⁹

* * *

Thank you for consideration. Please do not hesitate to contact us with any questions or for more information.

Harley Geiger
 Director of Public Policy
 Rapid7
 100 Summer Street, 13th Floor
 Boston, MA 02110
 617-247-1717

⁸ National Conference of State Legislatures, Data Security Laws, State Government, Jan. 16, 2017, <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx>.

⁹ See, e.g., Florida Stat. 501.171(4)(b).



March 7, 2018

The Honorable Blaine Luetkemeyer
 Chairman
 House Committee on Financial Services
 Subcommittee on Financial Institutions
 and Consumer Credit
 Washington, DC 20510

The Honorable William Lacy Clay
 Ranking Member
 House Committee on Financial Services
 Subcommittee on Financial Institutions
 and Consumer Credit
 Washington, DC 20510

RE: Hearing on "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

Dear Chairman Luetkemeyer and Ranking Member Clay,

The Society of Independent Gasoline Marketers of America ("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 but not limited to travel plazas, traditional "gas stations," convenience stores with gas pumps, cardlocks, and unattended public fueling locations.

Data security is deeply important to SIGMA's members and the customers they serve. To ensure that federal data security and breach notification legislation is as effective and fair as possible, SIGMA urges the Committee to follow four essential principles in designing a regulatory structure for data security and breach notification: First, data security and breach notification requirements must apply uniformly nationwide. Second, data security standards should be reasonable and adaptable to different types of businesses. Third, a fair and effective FTC enforcement regime should be maintained. Finally, data breach notification requirements apply across the board to businesses in all sectors of the American economy.

These principles have informed SIGMA's review of draft legislation circulated by Chairman Luetkemeyer and Representative Carolyn Maloney. Our review has raised concerns that the draft legislation does not meet these principles or fundamental standards of fairness and efficacy.

First, the draft bill fails to require all types of businesses to provide notice of their data breaches. Some businesses, including "service providers," "third parties," and many financial firms, are exempted from notification requirements that would apply to other American businesses. These exemptions would weaken the current state of the law on data breaches. While most states already require these businesses to provide notice of their data breaches, the draft legislation would provide federal exemptions from notice and preempt any attempt by the states to require notice. The result will be secret breaches that no one hears about and reduced

incentives to have good data security (because the threat of exposure of that fact will be diminished).

SIGMA is particularly troubled by certain language in the draft bill that would effectively require a non-exempt business to take on notification obligations in an exempt business' stead. This language is unfair, especially when considered alongside other unbalanced provisions of the draft bill, including provisions that would, among other things, allow "service providers" to decline even to investigate the data breaches they experience.

The draft legislation would also impose an overly rigid, one-size-fits-all collection of required data security practices on a huge variety of businesses, which would be unworkable in many cases. Ultimately, no single list of specific data security requirements could be comprehensive enough to cover such a diverse business community. By including exceptions for certain firms, the draft bill recognizes this limitation implicitly. These fixed enumerated requirements should be removed in favor of a flexible, reasonable standard for data security practices.

Additionally, the draft bill would change the Federal Trade Commission's enforcement capabilities so that it could punish businesses and levy fines even before applicable standards are firmly established. It is fundamentally unfair to subject a business to sanctions when it has no way of knowing what it needed to do to avoid such sanctions.

SIGMA is also concerned about the potentially unachievable "immediate" notice standard that the bill would impose (which is not a previously employed legal standard); inappropriate requirements that some breach victims provide notice to other private businesses as if those businesses were regulators; and failure to provide exceptions for situations in which a strict immediate notification requirement may do more harm than good, such as in cases where law enforcement seeks to delay breach notification for investigative or security reasons.

Before the Committee proceeds to mark up the draft legislation, it should take time to work with affected parties to prevent possible unintended harmful consequences. SIGMA thanks Chairman Luetkemeyer and Representative Maloney for the consideration they have shown during the development of this legislation, and stands ready to assist both offices with revisions to the draft bill that would mitigate negative effects on SIGMA members and similarly situated businesses.

Sincerely,



Douglas S. Kantor

Counsel, Society of Independent Gasoline Marketers of America

cc: Members of the Committee on Financial Services



Proposed Hybrid Enforcement Mechanism Explained

1. Data Security Enforcement

Any federal data security standards would be enforced by an insurer's domiciliary state chief insurance regulatory official. A domiciliary chief insurance regulatory official is a term of art referring to the official in a state where an insurer is "incorporated or organized."¹¹ Therefore, in practice, the intent of the language is that an insurer's security framework and any violations of the state's security regulation would be reviewed and enforced by that company's domiciliary chief insurance regulatory official.

2. Data Breach Notification Enforcement

Any federal data breach notification standards would be enforced by the chief insurance regulatory official of any state where there are consumers who were materially harmed by the breach. The intent of the language is if an insurer suffers a breach, with consumers materially harmed in multiple states, then the chief insurance regulatory official in any state with affected consumers would have the authority to enforce the federal notification requirements.

3. Reinsurer Notice and Breach Enforcement

Both data security and breach notification standards would be enforced by a reinsurer's domiciliary chief insurance regulatory official.

Proposed Legislative Language

SEC. 5. ADMINISTRATIVE ENFORCEMENT.

(a) IN GENERAL. — Notwithstanding any other provision of law, section xx shall be enforced exclusively under—

State insurance law, in the case of any covered entity that is engaged in the business of insurance, —

- (A) For any provisions related to data security in this Act, by the applicable chief insurance regulatory official of the state in which the covered entity is domiciled; and
- (B) For any provisions related to notification to consumers affected by a data breach in the state, by the chief insurance regulatory official of the state.

- (i) For a covered entity acting as an assuming insurer, any provisions related to notification should be made solely to the applicable chief insurance regulatory official of the state where the covered entity acting as the assuming insurer is domiciled.

¹¹ NAIC Company Licensing Definitions, available at, http://www.naic.org/documents/industry_ucaa_definitions.pdf



Statement for the Record

House Committee on Financial Services

Subcommittee on Financial Institutions & Consumer Credit

Hearing titled "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

March 12, 2018

The American Council of Life Insurers (ACLI) is pleased to submit this statement expressing the views of the life insurance industry regarding data security. ACLI thanks Chairman Blaine Luetkemeyer (R-MO) and Congresswoman Carolyn Maloney (D-NY) for their leadership on this issue, the subcommittee for holding this important hearing on March 7th, and for the consideration of our views on data security.

The ACLI is a Washington, D.C.-based trade association with approximately 290 member companies operating in the United States and abroad. ACLI advocates in state, federal, and international forums for public policy that supports the industry marketplace and the 75 million American families that rely on life insurers' products for financial and retirement security. ACLI members offer life insurance, annuities, retirement plans, long-term care and disability income insurance, and reinsurance, representing 95 percent of industry assets, 93 percent of life insurance premiums, and 98 percent of annuity considerations in the United States.

On February 16th, 2018, Chairman Luetkemeyer and Rep. Maloney released a data security discussion draft titled "Data Acquisition and Technology Accountability and Security Act." ACLI supports national risk-based data security and breach notification standards that would be enforced by state insurance departments. Such standards will provide the same security protection for personal information of individuals across the country and ensure consumers receive clear, consistent notice regardless of where they live or the type of entity subject to the breach.

ACLI member companies also support provisions that avoid needlessly alarming consumers, by requiring notice only when a breach in the security of consumers' nonpublic personal information is likely to cause harm. Our members support provisions not requiring notice if consumers' nonpublic information is protected by encryption or some other means that makes the information unreadable or unusable.

ACLI is grateful that the discussion draft excluded the insurance industry as we held discussions to develop language regarding a federal enforcement mechanism. Subsequent to the hearing, ACLI has determined that it supports a state-based enforcement model. Specifically, ACLI members support a mechanism that provides for the domiciliary state

American Council of Life Insurers
101 Constitution Avenue, NW, Washington, DC 20001-2133
www.acli.com

insurance department's enforcement for any data security standards, and for individual state insurance department's enforcement of any breach notification standards where consumers are directly affected by a breach in that state.

The intent of the language regarding data security standards is that an insurer's security framework and any violations of the state's security regulation would be reviewed and enforced by that company's domiciliary chief insurance regulatory official. A domiciliary chief insurance regulatory official is a term of art referring to the official in a state where an insurer is "incorporated or organized." The intent of the language referencing data breach notification standards is if an insurer suffers a breach, with consumers materially harmed in multiple states, then the chief insurance regulatory official in any state with affected consumers would have the authority to enforce the federal notification standards.

As this process moves forward, we look forward to working with the subcommittee, as well as the full Committee, to address these issues and to ensure clear standards are implemented for the protection of consumers and with the support of the life insurance industry.

Thank you for convening this important hearing and for your consideration of the views of ACLI and its member companies.

February 28, 2018

The Honorable Paul Ryan
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, DC 20515

Dear Speaker Ryan and Leader Pelosi:

Banks and credit unions are good stewards of their customers' personal information and data, so taking responsibility for it, and protecting it, is a role that every financial institution takes seriously. In fact, banks and credit unions are mandated, by our regulators, to notify their customers in the event of a breach. Fortunately, credible tracking statistics¹ on data breaches indicate that financial institutions remain one of the safest places for consumer data to reside.

Recently, Chairman Blaine Luetkemeyer (R-MO) of the House Financial Institutions and Consumer Credit Subcommittee and Congresswoman Carolyn Maloney (D-NY) released a draft bill that would improve data security for consumers across the country. The goal of the bill is simple—raise the bar so that all companies protect data similar to how banks and credit unions protect their data, and create a common-sense standard to ensure consumers receive timely notice when a breach does occur.

The draft bill recognizes the strict regulatory oversight the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and National Credit Union Administration have over bank and credit union breach notification policies and over the standards used to safeguard customer data. As such, the bill does not require banks and credit unions to subscribe to a duplicate notification requirement. What the bill does do, however, is require companies that are not subject to any current federal requirement regarding breach notification to tell consumers when their information has been compromised. Essentially, it brings expectations for these other sectors up to a standard very similar to that currently in place for banks and credit unions.

Contrary to statements made recently by some retailer groups, banks and credit unions have long been subject to regulatory mandates that set rigorous data protection and breach notification practices for financial institutions to follow. In fact, federal regulators describe these notification obligations as “an affirmative duty” for which compliance is demanded, and are considered to be an element of fundamental Safety and Soundness for the overall banking system. In addition, it must not be overlooked that the financial

¹ See e.g., “2018 – Data Breach Category Summary,” Identity Theft Resource Center. Accessed at: <https://www.idtheftcenter.org/images/breach/2018/ITRCBreachStatsReportSummary2018.pdf>

industry is the only sector subject to ongoing examination to ensure compliance with these breach notice obligations.

The status quo is not working for American consumers. New breaches are seemingly uncovered daily, and banks and credit unions are doing their part by communicating with their customers of the breach, reissuing cards and enacting fraud mitigation measures. But no solution will work unless everyone has an obligation to take these steps.

Consumers are tired of having their information compromised, and they should be—the stakes are too high. The time for a national data security and notification standard is now, and the draft legislation set forth by Chairman Luetkemeyer and Congresswoman Maloney achieves that objective.

Sincerely,

American Bankers Association

Consumer Bankers Association

Credit Union National Association

Financial Services Roundtable

Independent Community Bankers of America

National Association of Federally Insured Credit Unions

The Clearing House Association

CC: Members of the U.S. House of Representatives

Statement of
Property Casualty Insurers Association of America (PCI)
Subcommittee on Financial Institutions and Consumer Credit
House Financial Services Committee
“Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory
Regime”
March 7, 2018

The Property Casualty Insurers Association of America (PCI) appreciates this opportunity to provide our views on the Discussion Draft being circulated by Rep. Luetkemeyer and Rep. Maloney to establish a national data security and breach notification standard. PCI is composed of nearly 1,000 member companies, representing the broadest cross section of insurers of any national trade association. PCI members write \$220 billion in annual premium, 37 percent of the nation's property casualty insurance. Member companies write 44 percent of the U.S. automobile insurance market, 30 percent of the homeowners market, 35 percent of the commercial property and liability market and 37 percent of the private workers compensation market.

PCI is a strong supporter of the state insurance regulatory system and the McCarran-Ferguson Act, which reserved regulatory authority over the business of insurance to the states. However, data security and breach risks are not specific to the insurance industry – they are risks that affect nearly all businesses. The business community nationwide, including the insurance industry, is currently subject to a patchwork of state laws on breach notification and some laws on data security. Those laws are not consistent and thus they not only present compliance challenges to businesses, but also sow confusion among consumers as to why their rights are different from those in neighboring states. PCI members strongly believe that it would be beneficial to insurers and, more importantly, to their customers to have a single, uniform security and breach notification standard so that insurance consumers will know what to expect in case of a breach regardless of where they are located.

The Discussion Draft’s substantive provisions on data security and breach notice requirements are sensible standards that would help protect consumers. The data security requirements are appropriately risk-based, and yet not so prescriptive as to be inflexible in the face of rapid technological change.

Breach notice requirements are triggered only when there is a reasonable risk that a breach has resulted in actual harm to the consumer, *i.e.*, when there is a risk of identity theft, fraud, or economic loss (some state laws require notices to consumers when there is no real risk of consumer harm, which is unhelpful to consumers and may even lead them to ignore breach notices). The definition of “personal information” is in line with mainstream state definitions. The Draft would also allow covered entities to allocate breach notification responsibility among contractors and service providers contractually.

PCI acknowledges and commends the National Association of Insurance Commissioners (NAIC) for its efforts to achieve uniformity by adopting a model law on data security, which is now under consideration in the states. While PCI approves of many provisions of the model, it addresses only data security and not data breach requirements and is somewhat less tailored than the standards in the Discussion Draft. Of particular concern is that the model does not, by its terms, constitute an exclusive state remedy for insurance data security and breach issues. While exclusive adoption of the model in all states would lead to a more uniform standard as applied to insurers, many states already have laws of general application on their books and state legislatures may balk at separate rules for insurers. For these reasons, PCI urges Congress to adopt uniform, national standards.

PCI recognizes that state law preemption provisions of the bill may be controversial. However, we consider them essential to any federal bill. If Congress were to pass federal standards without preempting state laws, the federal standards would simply constitute a duplicative layer of regulation that would only make the existing patchwork situation worse, not better.

As it is currently drafted, the Discussion Draft would not apply to insurers, but PCI understands that the drafters are still considering including insurers. PCI strongly supports including insurers in the bill because it would be helpful to insurers and their customers for the bill’s uniform standards to apply. Discussions have centered on how to structure the enforcement provisions applicable to insurers. Insurance is regulated at the state level, including consumer protection regulation, so the Committee should take care not to create a duplicative federal enforcer of consumer protection rules. PCI believes a workable model can be found in the Title V privacy provisions of the Gramm-Leach-Bliley Act (GLBA), which included data security requirements. Enforcement of those rules was left to the functional regulators of each type of financial institution. Under Section 505, enforcement is “[u]nder State

insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled. . .”¹

The NAIC responded to GLBA by adopting a model regulation that incorporated the substantive provision of the Title V privacy rules, and states that did not already have GLBA-compliant laws or regulations on their books subsequently adopted the model. In the 18 years since GLBA was enacted, this mechanism has worked well to ensure that privacy protections for insurance consumers are consistent with those applicable to other federally regulated financial institutions. Indeed, because GLBA included data security provisions, the Discussion Draft might be seen as building upon the existing GLBA regime with respect to financial institutions, including insurers. Because the statute invited states to act on their own authority (which they did) rather than pursuant to a federal grant of authority, this approach was interpreted at the time and since as one that is workable and avoids constitutional issues.

The Committee adopted a variation on this approach in the last Congress when it reported H.R. 2205, the Data Security Act of 2015. That bill included an insurance enforcement provision modeled on GLBA, but also added a requirement that, for insurance groups licensed in multiple states, the lead state reinsurance regulator would be the enforcer for the entire group. The NAIC assigns a lead state to each group and the most current list of lead state assignments can be found at <https://isiteplus.naic.org/leadState/publeadstate/pubLShtml>. Because the current trend in insurance regulation is to look to lead state regulators for insurance groups, PCI would prefer and strongly endorses this approach.

PCI has already engaged in constructive discussions with Committee staff and members about the insurance enforcement provisions of the Discussion Draft, and we stand ready to continue to assist the Committee in developing an appropriate approach. PCI commends Rep. Luetkemeyer and his staff on a very good Discussion Draft and looks forward to continuing to work with Committee members and staff to enact uniform national data security and breach standards.

¹ 15 U.S.C. § 6805(a)(6).

February 13, 2018

The Honorable Blaine Luetkemeyer
 Chairman
 House Committee on Financial Services
 Subcommittee on Financial Institutions and
 Consumer Credit
 Washington, DC 20510

The Honorable William Lacy Clay
 Ranking Member
 House Committee on Financial Services
 Subcommittee on Financial Institutions and
 Consumer Credit
 Washington, DC 20510

RE: Hearing on “Examining the Current Data Security And Breach Notification Regulatory Regime”

Dear Chairman Luetkemeyer and Ranking Member Lacy Clay,

The undersigned associations represent over a million businesses in industries that directly serve American consumers. Our organizations appreciate the Committee calling a hearing to examine the current data security and breach notification regulatory regime. Our members are committed to protecting their customers’ data with effective data security practices and take the risk of breaches of security very seriously. In addition to the financial services companies under the Committee’s jurisdiction and our members’ businesses, the rampant nature of threats to consumer data is a challenge for businesses of all kinds. This includes companies that support communications with consumers and facilitate the acceptance of their forms of payment, as well as for professional organizations, health care institutions and government agencies.

Every industry sector – whether consumer-facing or business-to-business – suffers data security breaches that may put consumer data at risk. Less well known, however, is that three sectors in particular account for more than half of all breaches (i.e., security incidents with confirmed data losses) according to the [2017 Verizon Data Breach Investigations Report](#): financial services (24.3% of all breaches); healthcare (15.3%); and the public sector (e.g., governmental entities) (12.4%). According to this report, well above 80% of all breaches in 2016 occurred *outside* of the industries represented by the signatories to this letter, whose businesses typically handle less sensitive data than the sectors accounting for most breaches.

To protect consumers comprehensively, wherever breaches occur, Congress should ensure that any federal breach notification law applies to *all* affected industry sectors and leaves no holes in our system that would enable some industries to keep the fact of their breaches secret. Under the breach legislation reported by the House Financial Services Committee last Congress, however, Equifax would have been exempt from the bill’s provisions along with banks, credit unions and other entities that qualify as “financial institutions” under the Gramm Leach Bliley Act (GLBA). The absence of breach notice requirements for entities accounting for roughly a quarter of all security breaches annually would have left millions of Americans unaware of their potential risks of financial harm and identity theft. The exemption of Equifax and other financial services companies from the requirements of that bill would have created particularly weak

public policy given that the same bill provided those companies with preemption from the requirements of state laws.

Considering the widespread risk of data breaches afflicting all American industries and our governmental institutions, there are four key principles we support in federal data security and breach notification legislation:

1. **Establish Uniform Nationwide Law:** First, with the fifty-two inconsistent breach laws currently in effect in 48 states and 4 federal jurisdictions, there is no sound reason to enact federal legislation in this area unless it preempts the existing laws to establish a uniform, nationwide standard so that every business and consumer knows the singular rules of the road. One federal law applying to all breached entities would ensure clear, concise and consistent notices to all affected consumers regardless of where they live or where the breach occurs. Simply enacting a different, fifty-third law on this subject would not advance data security or consumer notification; it would only create more confusion.
2. **Promote Reasonable Data Security Standards:** Second, data security requirements in a federal law applicable to a broad array of U.S. businesses should be based on a standard of reasonableness. America's commercial businesses are remarkably diverse in size, scope and operations. A reasonable standard, consistent with federal consumer protection laws applicable to businesses of all types and sizes, would allow the right degree of flexibility while giving businesses the appropriate level of guidance they need to comply. Legislation taking this approach also would be consistent with the data security standard now used by the Federal Trade Commission (FTC) and nearly all state laws that include data security requirements in their breach notification statutes.
3. **Maintain Appropriate FTC Enforcement Regime:** Third, federal agencies should not be granted overly-punitive enforcement authority that exceeds current legal frameworks. For example, absent a completed rulemaking, the FTC must bring an action requiring a business to stop behavior that the FTC deems to be a violation of law. The FTC cannot seek civil penalties until it establishes what a violation is. That process gives businesses notice of the FTC's view of the law and is fair given the breadth of the FTC's discretion to determine what is legal.
4. **Ensure All Breached Entities Have Notice Obligations:** Finally, businesses in every affected industry sector should have an obligation to notify consumers when they suffer a breach of sensitive personal information that creates a risk of identity theft or financial harm. Informing the public of breaches can help consumers take steps to protect themselves from potential harm. Moreover, the prospect of public disclosure of breaches creates greater incentives for all businesses handling sensitive personal information to improve their data security practices. Creating exemptions for

particular industry sectors or allowing breached entities to shift their notification burdens onto other businesses will weaken the effectiveness of the legislation, undermine consumer confidence, ignore the scope of the problem, and create loopholes that criminals can exploit.

We note that a group of organizations led by the Financial Services Roundtable (FSR) wrote to the House Energy and Commerce Committee on January 4, 2018, relaying the elements of legislation that those groups favor. The FSR letter advocated for a “flexible, scalable” data security standard that included factors such as the “size and complexity” of a business, the “cost of available tools to secure data,” the “sensitivity” of the information the company maintains, and “guarantees” that small businesses are not excessively burdened. The reasonableness standard endorsed by the FTC that the undersigned organizations support already meets all of those criteria. However, as soon as laws mandate specific data security requirements for businesses, they become inflexible and burdensome for smaller entities, and outdated and inadequate for larger or more sophisticated businesses. We appreciate that the FSR-led letter appears to agree with us on this point.

We are also pleased that the FSR-led letter appears to agree with our principle on breach notification requirements for entities handling information that, if breached, may cause individuals to become victims of financial harm or identity theft. Their letter calls for a “notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators.” In the past, this Committee’s breach legislation has exempted businesses in industries such as telecommunications, financial services, and data storage from required consumer notice when they are breached. That certainly would not meet the language of the FSR-led letter and is not acceptable to our organizations either. While some businesses subject to GLBA have asked for exemptions from notice obligations in new legislation, those requests raise significant problems given that GLBA does not require breach notification.¹ No industries are exempt from the attention of data thieves and no industries should be exempt from a statutory requirement to provide notice to consumers when they have breaches. Legislation should not serve as cover for giving breached businesses the ability to keep secret their own breaches and the risks of harm to affected individuals.

The four principles above, which are supported by the undersigned organizations, are important to ensure that any data security and breach notification legislation advanced in Congress does not overly burden business already victimized by a breach, does not impose unfair burdens on unbreached entities, and does not pick regulatory winners and losers among differing business sectors in the process. We urge you to exercise your leadership to find legislation that can meet these four principles. Additionally, any such process needs to include input from all affected industries and from businesses of all sizes. Otherwise, it risks imposing unfair or

¹ GLBA’s statutory language, approved by Congress in 1999, predates the first state breach notification law by several years and does not actually require notification of security breaches. Regulatory guidelines implementing GLBA adopted in 2005 recognized this omission, but did not correct it. Rather, the guidelines state that GLBA-covered entities “*should*” make breach notice, but notice is discretionary and not a *requirement*. Legislation exempting GLBA-covered entities therefore leaves them without a notice requirement.

crippling burdens on some sectors but not others, which, unfortunately, has been the case with several past legislative proposals.

We appreciate your consideration of our views as on this hearing and we look forward to a continued constructive dialogue with you on these matters.

Sincerely,

American Hotel & Lodging Association
International Franchise Association
National Association of Convenience Stores
National Association of Realtors
National Association of Truck Stop Operators
National Council of Chain Restaurants
National Grocers Association
National Restaurant Association
National Retail Federation
Society of Independent Gasoline Marketers of America
U.S. Travel Association

cc: Members of the U.S. House of Representatives



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

May 11, 2018

Via email to Terrie Allison,
Financial Services Committee Editor
(Terrie.Allison@mail.house.gov)

The Honorable Maxine Waters
Ranking Member
The Committee on Financial Services
U.S. House of Representatives
Washington, DC 20215

The Honorable Dennis A. Ross
Subcommittee on Financial Institutions and
Consumer Credit,
The Committee on Financial Services
U.S. House of Representatives
Washington, DC 20215

Re: *Financial Institutions and Consumer Credit Subcommittee's March 7, 2018
Hearing: Legislative Proposals to Reform the Current Data Security and Breach
Notification Regulatory Regime*

Dear Ranking Member Waters and Representative Ross:

Thank you for your questions regarding certain provisions of the Discussion Draft entitled, "Data Acquisition and Technology Accountability and Security Act" (the "DD"). We appreciate the opportunity to respond and hope these responses are helpful to the Subcommittee as it considers the Discussion Draft.

I. QUESTIONS FROM RANKING MEMBER WATERS

A. Preemption of State Law¹

- *As this Committee considers creating national data security and breach notification standards, can you comment on whether you believe it is critical that we preserve the ability of states to protect their residents from emerging threats to the privacy and security of their data?*
- *Why is it important that we continue to preserve the states' ability to address emerging data security vulnerabilities and quickly amend consumer protections to address any new threats that emerge?*

¹ Please note that in order to provide more comprehensive responses, we grouped certain questions of Ranking Member Waters into the subject areas reflected in the sub-headers preceding each set of questions and responses.



- *What are the consequences of the scope of state preemption as outlined in Section 6 of the DD?*

We believe it is critical to preserve the ability of the States to protect their residents from the emerging threats to their data privacy and security. The States have been on the front lines of the cybersecurity problem, utilizing both their existing consumer protection authority and enhancing those protections by enacting new laws in response to the evolving nature of data security risks.

Section 6 would undercut this progress. As drafted, its effect would be to preempt Massachusetts' existing data breach notification law and data security standards (Mass. Gen. Law c. 93H and 201 CMR 17.00, respectively), as well as all those of other states. It would wipe clean state legislative regimes that have been protecting consumers for nearly a decade, and replace them with a less protective standards set forth in the DD.

It would also interfere with important and ongoing state legislative activity in this area. In the wake of the Equifax breach, at least 30 states have proposed or enacted legislation to enhance existing state data protections for consumers.² The Massachusetts Legislature is no exception and is currently advancing a package of important reforms (discussed further below), to give Massachusetts consumers more protections after a breach. Section 6 would interfere and undermine these important legislative efforts.

Section 6 further erects a barrier to a State's ability to enforce civil and criminal laws that protect consumers from risks other than a data breach. As drafted, the reach of section 6 could extend to a variety of other state laws apart from strictly data breach notice laws, to the extent such laws are found to concern "securing information from unauthorized access or acquisition of data." States rely on a variety of civil and criminal laws to protect their consumers' "information" from threats, including, for example, state consumer protection laws (*see, e.g.*, Mass. Gen. Law c. 93A), state laws that protect medical records and mental health records from unauthorized access (*see, e.g.*, Mass Gen. Law c. 111, § 70E(b), and c. 123, § 36), or even criminal laws against identity theft or cybercrime. *See, e.g.*, Mass. Gen. Laws c. 266, § 37E.

In sum, we believe that the restrictive "ceiling" on consumer protection imposed by the DD will leave consumers in a worse position than the status quo. Because data security risks continue to evolve rapidly, the States must be free to innovate and act quickly to best protect the needs of their residents. Instead of an inflexible federal security and breach standard that may not keep up with changing technologies, a federal standard should set only a "floor" of protections that state law is free to exceed.

² *See* National Conference of State Legislatures, *2018 Security Breach Legislation*, at <http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx> (listing state legislation and noting that "since the Equifax data breach in 2017, a number of states introduced legislation that would provide for free credit freezes for victims of data breaches or that are otherwise aimed at credit bureaus or financial institutions. Other bills would amend breach laws to expand the definition of 'personal information,' to set specific timeframes within which a breach must be reported, or require reporting to the state's attorney general. In addition, several bills would require notification in the case of breaches of student information.").

B. *Breach Notification - Timing*

- *The DD provides that a written, telephonic, email or substitute notice of a breach must be provided to a consumer if the breached entity determines that there is a reasonable risk that the breach of data security has resulted in ID theft, fraud or economic loss to any consumer. ...*
 - *[D]o you agree that the standard leaves open the possibility of a generous interpretation and, thus, a delay of the eventual notification to consumers, as well as giving excess leeway for “covered entities”, if and when litigation is involved?*
 - *What express timing standard would you suggest replacing this standard with, and do you agree that explicitly providing a time period, such as 72 hours, would provide less unwarranted leeway and hold the covered entities accountable to both law enforcement and consumers?*
 - *Lastly, can you provide any additional comments on why the notice provisions in Section 4 of the DD are insufficient to protect consumers?*
- *Can you comment on the “without unreasonable delay” standard, as stated in Section 4(b)(1) under the DD, to be applied when providing notice to law enforcement of a breach following a preliminary investigation?*

Notifying consumers as soon as possible after the breach is critical to prevent the various consumer harms that can result. Prompt notice allows the consumers to take the steps that are necessary to protect themselves from resulting harms, such as identity theft. We believe that the notice provisions of the DD (section 4(b)(2)) do not achieve this goal.

First, by its own terms, the DD does not require that consumers be notified until after the entity determines that the breach “has [already] resulted in identity theft, fraud, or economic loss to” the consumer. This is too late. Notifying a consumer only after they have been harmed deprives the consumer of any opportunity to avoid identity theft and fraud, and thus is ineffective and unfair.

The DD also creates perverse incentives for an entity to delay or even avoid providing any consumer notice—even with regard to breaches that do result in documented consumer harm. Section 4 of the DD requires an entity to conduct a “preliminary investigation” before providing consumer notice, but it provides no outer time limit for such an investigation. *See* section 4(a), (b)(1). The lack of an outer time limit for the preliminary investigation creates the risk that an entity would use its preliminary investigation as a pretext to delay notifying consumers (thereby putting them at a higher risk of harm) for its own strategic purposes. Further, nothing in the DD explicitly requires an entity to engage in any analysis of whether any given breach “has resulted in identity theft, fraud, or economic loss” to any given consumer. Because of the difficulty in connecting a particular breach to a particular instance of consumer harm (even more so due to the Equifax breach, which put nearly half of the country at a heightened risk of identity theft), a covered entity can simply opt to not engage in the analysis as a way to avoid triggering any consumer notification duty.

This approach is a drastic departure from the data breach laws of virtually every state. State data breach laws almost universally require consumer notice before the accrual of any resulting harm, which gives consumers the best chance to mitigate the consequences of the breach. Further, virtually every state requires consumer notice “as soon as practicable,” in “the most expedient time possible,” “without unreasonable delay,” or functionally equivalent language, after the discovery of a breach, even if they also require an entity to conduct a preliminary investigation.³ Finally, because the circumstances of each breach vary widely, the vast majority of the States have opted not to impose outer time limits for notice to consumers.⁴

The States’ approach to this issue is the better one. Replacing state laws with the less protective standards currently proposed in the DD will leave consumers less protected, and at an increased risk of harm.

³ See Alabama, 2018 S.B. 318, Act No. 396; Alaska Stat. § 45.48.010 *et seq.*; Ariz. Rev. Stat. § 18-545; Ark. Code § 4-110-101 *et seq.*; Cal. Civ. Code §§ 1798.29, 1798.82; Colo. Rev. Stat. § 6-1-716; Conn. Gen. Stat. § 36a-701b; Del. Code tit. 6, § 12B-101 *et seq.*; Fla. Stat. § 501.171; Ga. Code § 10-1-910, -911, -912; Hawaii Rev. Stat. § 487N-1 *et seq.*; Idaho Code § 28-51-104 *et seq.*; 815 Ill. Comp. Stat. 530/1 *et seq.*; Ind. Code § 24-4.9-3-3; Iowa Code § 715C.1 *et seq.*; Kansas Stat. § 50-7a01 *et seq.*; Ky. Rev. Stat. § 365.732; La. Rev. Stat. § 51:3071 *et seq.*; La. Admin. Code tit. 16, pt. III, § 701; Me. Rev. Stat. tit. 10, § 1346 *et seq.*; Maryland Code Ann., Com. Law. § 14-3501 *et seq.*; Mass. Gen. Laws. c. 93H, § 3; Mich. Comp. Laws § 445.72; Minn. Stat. § 325E.61; Miss. Code, Title 75, § 75-24-29; Mo. Rev. Stat. § 407.1500; Mont. Code § 30-14-1701 *et seq.*; Neb. Rev. Stat. 87-803; Nev. Rev. Stat. § 603A.010 *et seq.*; N.H. Rev. Stat. Ann. § 359-C:19 *et seq.*; N.J. Stat. Ann. § 56:8-163; 2017 H.B. 15, Chap. 36 (effective 6/16/2017); N.Y. Gen. Bus. Law § 899-aa; N.C. Gen. Stat. § 75-60 *et seq.*; N.D. Cent. Code § 51-30-01 *et seq.*; Ohio Rev. Code § 1349.19; Okla. Stat. tit. 24, § 161-166; Or. Rev. Stat. § 646A.600 *et seq.*; 73 Pa. Stat. §§ 2301-08, 2329; R.I. Gen. Laws §§ 11-49.2-3 – 11-49.3-6; S.C. Code § 39-1-90; South Dakota, 2018 S.B. 62; Tenn. Code § 47-18-210; Tex. Bus. & Com. Code § 521.053; Utah Code 13-44-101 *et seq.*; Vt. Stat. Tit. 9, §§ 2430, 2435; Va. Code § 18.2-186.6; Wash. Rev. Code. § 19.255.010 *et seq.*; W. Va. Code § 46A-2A-101 *et seq.*; Wis. Stat. § 134.98; Wyoming Statutes 40-12-d501 *et seq.*

⁴ Eleven states include express outer time limits for consumer notice, generally ranging from 30–90 days, while still requiring notice sooner if practicable. See Conn. Gen. Stat. § 36a-701b (2017) (“without unreasonable delay but not later than ninety days”); Fla. Stat. § 501.171 (2017) (“as expeditiously as practicable, but no later than 30 days after the determination of a breach or reason to believe a breach occurred”); Md. Code Ann., Com. Law § 14-3504 (LexisNexis 2017) (effective Jan. 1, 2018) (“as reasonably practicable, but not later than 45 days after the business concludes the investigation”); N.M. Stat. Ann. § 57-12C-6 (LexisNexis 2017) (“most expedient time possible, but not later than forty-five calendar days following discovery of the security breach”); Ohio Rev. Code Ann. § 1349.19 (LexisNexis 2017) (“in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system”); 11 R.I. Gen. Laws, § 11-49.3-4 (2017) (“in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements”); South Dakota, 2018 S.B. 62 (“not later than sixty days from the discovery or notification of the breach of system security. . .”); Tenn. Code Ann. § 47-18-2107 (2017) (“no later than forty-five (45) days from the discovery or notification of the breach of system security”); Vt. Stat. Ann. tit. 9, § 2435 (2017) (“in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification”); Wash. Rev. Code § 19.255.010(16) (2017) (“in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered”); Wis. Stat. § 134.98(3)(a) (2017) (“within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information”).

C. *Breach Notification - Financial Harm Triggers*

- *The [DD] requires that “if, after completion of [a] preliminary investigation” a covered entity determines “that there is a reasonable risk that the breach of data security has resulted in identity theft, fraud, or economic loss to any consumer, the covered entity shall immediately notify such consumer, without unreasonable delay.” Can you comment on why consumers may want to be notified about a breach even if the breached entity doesn’t believe that it “has resulted in identity theft, fraud or economic loss” to a consumer?*
- *The DD provides that a written, telephonic, email or substitute notice of a breach must be provided to a consumer if the breached entity determines that there is a reasonable risk that the breach of data security has resulted in ID theft, fraud or economic loss to any consumer. Can you comment on the other types of harm that may result from a breach that would not require a covered entity to provide notice to a consumer?*
- *Why is “financial harm” not the right trigger for requiring consumer breach notification? What trigger best protects consumers?*
- *Why is “financial harm” not the right trigger for requiring consumer breach notification? What trigger best protects consumers? How many states are you aware of that do not have any form of harm trigger in place?*

Consumers must be notified of a breach precisely so that they may take steps to avoid resulting harms. The “financial harm trigger” in the DD risks depriving the consumer of this critical window of opportunity. Indeed, because connecting any specific breach to financial harm is a difficult and time consuming process, a breached entity may not have the necessary information (or the incentive) to effectively judge the risk of harm created by the breach as to any given consumer and fail to notify consumers where such notice is warranted.

Financial harm triggers by definition fail to take into account non-financial harms, such as medical identity theft, professional or personal embarrassment, or loss of access to online accounts or services. A consumer could suffer harm to his or her reputation, or even face blackmail, if private information accessible via the stolen personal information were made public.⁵ And in reacting to the breach, consumers suffer various other non-financial harms, such as stress and anxiety due to their increased risks of identity theft and fraud, and time and energy spent monitoring accounts, closing accounts and credit reports, placing security freezes or fraud alerts, among other measures, necessary to protect themselves from the consequences of the breach. These harms, among others, are no less damaging to the individual consumer than a financial loss, and in fact may be worse to the extent they are incapable of financial redress.

⁵ The U.S. Commerce Department’s National Institute of Standards and Technology has also recognized that such non-financial harms can result from the unauthorized access of personally-identifiable information. See Erika McCallister, Tim Grance, & Karen Scarfone, “Guide to Protecting the Confidentiality of Personally Identifiable Information (CPU),” NIST Special Publication 800122, at ES1 (2010), available at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800122.pdf>.

Finally, financial harm triggers undercut another important purpose of a public data breach notice regime: data breach notice laws create a powerful incentive to implement and maintain strong data security safeguards to prevent the breach in the first place.

A better approach is to require breach notification as soon as reasonably practicable and without unreasonable delay when an entity knows, or has reason to know, that protected personal information of a consumer has been acquired without authorization, or used for unauthorized purposes. In other words, notice should be triggered by the breach itself; not later, when the breach results in harm to the consumer. This is the approach taken by at least 9 states and the District of Columbia.⁶ Twenty-six other states that do have a harm trigger for consumer notice take into account non-financial harms.⁷ The DD's financial harm trigger is contrary to the majority of the State's laws and would leave consumers less protected than today.

D. Third Party Obligations

- *Under DD, a "third party" means any entity that "processes, maintains, stores, or handles, or otherwise is permitted access to personal information in connection with providing services to a covered entity. The DD mandates that if a third party becomes aware that a breach of data security involving data in electronic form containing personal information that is maintained, or otherwise handled on behalf of a covered entity, has or may have occurred, the third party would be required to take the following steps to investigate the scope and nature of the breach, notify the covered entity whose data may have been compromised, and cooperate with the covered entity in resolving the incident.*
 - *Although this clause mandates actions by third parties, there are no explicit guidelines in setting up compliance processes for this group that would allow for the potential identification of areas of high risk, and thus prime for data breaching. In addition, the DD fails to specify the time in which a third party must notify the covered entity, the language simply asks they notify the covered entity.*
 - *At this point, we are already one step removed from the consumer, as any delay by the third party will then ultimately be paid by the consumer awaiting notice by their covered entity. Can you please comment on this?*

⁶ See Cal. Civ. Code § 1798.29; 815 Ill. Comp. Stat. § 530/10; Mass. Gen. Laws c. 93H, § 3; Minn. Stat. § 325E.61; Nev. Rev. Stat. § 603A.220; N.Y. Gen. Bus. Laws § 899aa; N.D. Cent. Code § 51-30-01, 51-30-02; Tex. Bus. & Com. Code § 521.05; D.C. Code § 28-3852.

⁷ See Alaska Stat. § 45.48.010; Ark. Code Ann. § 4-110-105; 2 Colo. Rev. Stat. § 6-1-716; Conn. Gen. Stat. § 36a-701b; Del. Code tit. 6, § 12B-102; Haw. Rev. Stat. § 487N-1; Idaho Code Ann. § 28-51-105; La. Rev. Stat. Ann. § 51:3074; Me. Rev. Stat. Ann. tit. 10, § 1348; Md. Code Ann. Com. Law § 14-3504; Mich. Comp. Laws § 445.72; Miss. Code Ann. § 75-24-29; Mont. Code Ann. § 30-14-1704; Neb. Rev. Stat. § 87-803; N.H. Rev. Stat. Ann. § 359-C:20; N.J. Stat. Ann. § C.56:8-163; N.C. Gen. Stat. §§ 75-61; 75-65; Or. Rev. Stat. § 646A.604; 73 Pa. Stat. Ann. § 2302; S.C. Code Ann. § 1-11-490; Tenn. Code Ann. § 47-18-2107; Utah Code Ann. § 13-44-202; Vt. Stat. Ann. § 2435; Wash. Rev. Code § 19.255.010; Wyo. Stat. Ann. § 40-12-502.

It is critical that any data breach law clearly allocate responsibilities for providing consumer notices among the ultimate owner of the breached personal information and a third party custodian when information is breached. Unambiguous allocation of notice obligations ensures that notice to consumers is not delayed because of private disputes among the parties as to who must send notice.

Massachusetts, like its sister states, addresses this concern by defining third parties by their legal relationship to the breached data: i.e. entities that “maintain[] or store[], but do[] not own or license” the breached information. It then requires those entities to provide notice of the breach “as soon as practicable and without unreasonable delay” to the “owner or licensor of the information,” who in turn notifies consumers and state agencies. Mass. Gen. Laws c. 93H, § 3(a), 3(b).

By contrast, the DD’s definitions of a “covered entity” and a “third party” rely on overlapping descriptions of how each handles the breached personal information.⁸ Such ambiguity appears likely to fuel private disputes over which entity bears the notification duty (especially in cases where both entities are providing services to the other), with resulting delays in consumer notice.

The lack in section 4 of any time limit for third parties to notify the covered entity of the breach further creates the opportunity for delays at the very start of the notification process, delays that only increase as the notified entity engages in its preliminary investigation required by section 4(a). The risk of such delays should not be borne by the consumer. Because of this concern of delay, the data breach laws of at least 18 states require that third parties notify the owner/licensor of the breached information “immediately” following the discovery of the breach.⁹

We urge the Subcommittee to consider clarifying the responsibilities for providing consumer notice as between third parties and covered entities, and requiring the third party to notify the covered entity either “immediately” or “in the most expeditious time possible” upon discovery of a data security incident.

E. Credit Freezes and Locks

- *In the wake of the massive Equifax breach that exposed the personal information of more than 148 million Americans, your boss, State Attorney General for the Commonwealth of*

⁸ The DD defines a “covered entity” as one that “accesses, maintains, or stores personal, or handles personal information,” (Sections 2(7) and 4(b)(2)). It similarly defines a “third party” as one that “processe[s], maintain[s], stores, or handles, or otherwise is permitted access to personal information in connection with providing services to a covered entity” (Section 2(11)(A)).

⁹ See Colorado (Col. Rev. Stat. Title 6, Article 1, §6- 1-716(2)(b)); Connecticut (Conn. Gen. Stat. §36a-701b(c)); Delaware (Del. Code tit. 6 § 12B-102(b)); Hawaii (Hawaii Rev. Stat. §487N-2(b)); Iowa (Iowa Code § 715C.2(2)); Minnesota (Minn. Stat. § 325E.61(b)); Missouri (Mo. Rev. Stat. § 407.1500(2)(2)); Montana (Mont. Code § 30-14-1704(2)); New Hampshire (N.H. Rev. Stat. Ann § 359-C:20(1)(C)); Nevada (Nev. Rev. Stat. § 603A.220(2)); New York (N.Y. Gen. Bus. Law § 899-aa(3)); North Carolina (N.C. Gen. Stat. § 75-65); North Dakota (N.D. Cent. Code § 51-30-03); South Carolina (S.C. Code § 39-1-90(B)); Texas (Tex. Bus & Com. Code § 521.053(c), Utah (Utah Code 13-44-202(3)(a), Vermont (Vt. Stat. Tit. 9, § 2435(b)(2)); and Washington State (Wash. Rev. Code § 19.255.010(2)).

Massachusetts Healey, along with a number of other Massachusetts legislators, announced the introduction of legislation to increase consumer access to credit freezes, prohibit consumer reporting agencies from charging consumers to suspend, or remove such freezes, and ensure free access to credit monitoring services. Can you discuss why your office believes that these reforms are so critical?

The Equifax data breach compromised the most sensitive personal information of nearly 3 million Massachusetts consumers. It is the worst data breach the Commonwealth has seen in a decade, both because of its scope and because of the central role that Equifax plays in the financial services industry. We therefore acted quickly to hold Equifax accountable by filing a state enforcement action under our state data breach and data security laws and our consumer protection law.

The Equifax breach also revealed that consumers need more control over who obtains access to personal information held by credit reporting agencies, an area of concern not directly addressed by existing state or federal law. In partnership with state legislators, we proposed several enhancements to the Commonwealth's consumer protection laws in September 2017 to provide additional tools for consumers to control who has access to their credit, and to take remedial action when that information falls into the hands of unscrupulous parties. We are pleased to report that the Massachusetts House of Representatives approved a bill in February 2018, and the Massachusetts State Senate advanced a bill in April 2018.

Both versions provide for the enhanced consumer protections that are critical after the Equifax breach:

- **More consumer control over credit reports.** Consumers need more transparency and control over who accesses their credit files, when, and for what purposes. Currently, consumers' credit files are accessible by default to entities with a "permissible purpose" under the Fair Credit Reporting Act. The consumer has few tools to limit or monitor third parties' access to that information¹⁰. We believe that consumers should have the right to decide who sees their credit files. Both the House and Senate bills thus require written consent before third parties can access a consumer's credit report.
- **Free credit freezes for all Massachusetts consumers.** Current state law allows the consumer reporting agencies to charge \$5 to place, suspend and revoke a freeze. After its breach, Equifax temporarily waived the costs of placing a freeze, but Experian and Transunion continued to charge consumers. The bills would make the placement, thawing, and lifting of security freezes free for all consumers.
- **Faster Freezes.** Both bills codify a requirement that consumer reporting agencies must comply with a freeze request in no less than a day, and would have to

¹⁰ Those tools include credit freezes, proprietary credit "locks," opt-outs from pre-screened offers of credit, 90-day fraud alerts and free credit reports available under state or federal law. See 15 USC 1681i(b)(4)(E) (three free credit reports under federal law); 15 USC 1681j(a) (three free credit reports per year under Massachusetts law).

temporarily suspend or permanently remove a freeze in just 15 minutes, if the request to place, lift or remove the freeze is made electronically.

- **“One-Stop Shop” for Credit Freezes.** Consumers have expressed deep frustration about placing security freezes after the Equifax breach, since each agency had its own website and process, potentially leading some not to take advantage of this important protection. The House and Senate bills, with some differences, envision a “one-stop-shop” that allows consumers to find information in one place about how to place a credit freeze. The Senate version requires the agencies to establish an electronic mechanism that permits consumers to place a freeze once, triggering a freeze at all three agencies. This “one-stop-shop,” along with the prohibition on fees for credit freezes, is intended to remove undue burdens on consumers whose personal information has been compromised by a breach, and to give consumers more control over access to their credit profile.
- **Free Credit Monitoring.** Both branches endorsed proposals to require free credit monitoring for consumers impacted by a breach of personal information. The Senate bill requires that if a consumer reporting agency is itself breached, it must provide at least five years of free credit monitoring. This provision recognizes that identity thieves may not use unlawfully obtained information immediately after the breach. Further, it removes the ability of a credit reporting agency to profit by charging affected consumers for credit monitoring services necessitated by its own breach.

The House and Senate have established a conference committee to resolve the technical and substantive differences between the two bills. The Massachusetts Legislature concludes its formal sessions on July 31, 2018. We are hopeful that these new mechanisms will also encourage consumer reporting agencies to be more diligent about protecting consumers’ data, and give our consumers more assurances that their private data is better protected.

F. Gramm-Leach-Bliley Act

- *As you know, the Federal Trade Commission (FTC), which has jurisdiction for implementing the Gramm-Leach-Bliley Act Safeguards Rule for non-bank financial institutions, does not have supervisory authority, and therefore cannot regularly verify whether businesses subject to its requirements are actually implementing and adhering to adequate data security measures. This means that companies like, Equifax, TransUnion, and Experian, are not subject to exams for their data security practices, despite the fact that they hold vast troves of the most sensitive consumer data. Does this gap in regulatory oversight concern you? Does it concern you, therefore, that the DD does nothing to strengthen enforcement of the Safeguards Rule, particularly for entities that fall under the ambit of the FTC?*
- *Would you support a requirement that consumer reporting agencies be required to register with a federal regulator and be subject to comprehensive, and regular, examinations to assess the adequacy of their data security protocols?*

We think there is merit to exploring greater federal oversight of consumer reporting agencies, including regular review of their policies and procedures for protection of consumers' personal information. Given the central role that consumer reporting agencies play in the economy and the amount of sensitive personal information they handle, gaps in their data security posture should be identified and addressed well before they result in a breach.

G. Credit Reporting Reforms

- *Where do you think Congress should start in overhauling the broken credit reporting industry? What are some of the most impactful reforms that Congress could enact, such as reforms to improve accuracy of credit files, limiting the use of credit information for employment decisions, empowering regulators to oversee the development of credit scoring models, cracking down on deceptive marketing, increasing consumers' access to free credit reports, scores, and identity theft protection tools?*

We agree that the current federal regime governing the credit reporting system is ripe for review in light of the new threats to consumers' data privacy and security raised by the digital economy, including with respect to the areas of concern outlined in this question.

The legislation we propose in Massachusetts is intended to lower barriers for consumers to protect themselves from harm that might result from a data breach. Further enhancements, such as more frequent access to or control over credit reports, or giving consumers the ability to opt-out of the credit reporting system entire, are hindered by federal law, in particular 15 U.S. Code § 1681t.

If Congress expands preemptive language in federal law, it will freeze in place protections that are incapable of addressing future data privacy and security risks. Massachusetts, like many of its sister states, has benefitted from a Legislature that is engaged and fluent in data security. We thus urge members of the Subcommittee to carefully evaluate proposals that could further inhibit the States' authority in this space. Instead, Congress should preserve the States' ability to enact innovative, effective and comprehensive consumer protections in this arena.

- *At a "Minority Day" hearing called by the Democrats of this Committee held last year, we heard extensive testimony outlining the inexcusable culture of impunity and exploitation among the nation's largest consumer reporting agencies. Given this, I would like to get your views on how Congress should hold this industry accountable and protect consumers. To get a sense of the steps you think Congress should be considering, please answer yes or no to the following questions:*
 - *Should this Committee explore an explicit "opt-out" to allow consumers to block certain consumer reporting agencies acquiring and selling their sensitive personal and financial information?*

Yes. The Committee should explore giving consumers more control over who can access the personal information collected, held and sold to third parties by the consumer reporting agencies.

- *Should consumer reporting agencies be required to register with a Federal regulator, and be subject to comprehensive regular examinations covering their*

obligations under the Fair Credit Reporting Act as well as their data security obligations under the Gramm-Leach-Bliley Act?

Yes. As discussed above, we think there is merit to exploring greater federal oversight of consumer reporting agencies, including regular review of their policies and procedures for protection of consumers' personal information.

- *Should Congress explore whether in extreme cases it makes sense to shut down companies like Equifax, that fail to implement basic protections to safeguard consumer information?*
- *Are the tools to hold consumer reporting agency executives accountable sufficient, or should Congress strengthen tools that would allow regulators to claw back executive pay, ban abusive and negligent bad actors from the industry, or even impose criminal penalties as appropriate?*

As a general matter, we think federal regulators should have robust tools to ensure consumer reporting agencies are acting responsibly with consumers' data, including by protecting that data from known risks. This is especially true where a consumer reporting agency relies primarily on business-to-business transactions, not the sale of consumer services or products (where the fear of losing consumer goodwill might provide some deterrent to bad practices).

II. QUESTIONS FROM REPRESENTATIVE ROSS

1. *Do you understand the Data Acquisition and Technology Accountability and Security Act to apply exclusively to data stored electronically? Or, would paper files held by covered entities also be subject to the bill's requirements? Are there any concerns with clarifying at the outset that this bill applies only to data stored electronically?*

No. We do not read the DD as applying to electronic records only. The definitions of "personal information" and "breach of security" are silent as to whether the data at issue are paper or electronic. Similarly, the requirements of section 3 ("Protection of Information") and section 4 ("Notification of Breach of Data Security") are not expressly limited to electronic data.

Data can be breached no matter its form. The Massachusetts data breach law covers personal information in both electronic and paper form. In our review of over 21,000 data breaches reported to our office over the past decade, we have seen numerous breaches of paper files, including (as just some examples): the mass mailing of employee wage statements or benefit information to the wrong parties, or the printing of social security numbers within the address line of those mailings, the abandonment of legal files in public places,¹¹ the unauthorized access

¹¹ See *Commonwealth of Massachusetts v. Haney*, Case No. 1684CV00018 (Jan. 15, 2016, Suffolk Superior Court) (consent judgment entered against lawyer for violations of Massachusetts data protection law for abandoning intact legal files containing the unredacted social security numbers and mortgage information of consumers in a field next to a public footpath).

of consumer paper files by a rogue employee; or the disposal of intact consumer records in public dumps.¹²

Such breaches are no less concerning or harmful to the individual consumer than a breach of electronic files and it is just as important that consumers are notified when they occur.

2. *Under the discussion draft, customer notification is required “immediately” unless it’s delayed at the instruction of law enforcement. Can you explain how codifying a specific timeframe may negatively impact customers or an investigation by law enforcement? Do you believe there are standards other than “immediate” that would be better? If so, please explain why. Do you have any other suggestions for how this standard could be improved?*

Section 4(b)(2) of the DD requires that consumers be notified “immediately,” but only after the entity has already conducted the preliminary investigation outlined in section 4(b)(1). As noted above, because the circumstances of each breach are context-dependent, Massachusetts, like the vast majority of the States, has opted not to impose outer time limits for notice to consumers. *See supra*, note 3. Instead, Massachusetts requires that notice be issued “as soon as practicable and without unreasonable delay” when the entity “knows or has reason to know” of a breach. Mass. Gen. Laws c. 93H, § 3(b). Massachusetts also permits a delay in consumer notice if that delay is requested by law enforcement. *Id.* § 4. The majority of states follow a similar approach. *See supra*, note 3.

- a. *Can you provide me an example of a legal standard requiring “immediate” notification in any other provision of law and explain to me how anyone meets that requirement?*

The data breach laws of at least 18 states require third parties to notify the owner/licensor of the breached information “immediately” following the discovery of the breach. *See supra*, note 9. Immediate notification of incidents that threaten public health or welfare is further required by various federal laws and regulations. *See, e.g.*, 30 CFR 50.10 (requiring mine operators to “immediately contact [the federal Mine Safety and Health Administration] at once without delay and within 15 minutes at the toll-free number . . . once the operator knows or should know that an accident” involving a mine worker has occurred); 33 CFR 173.53 (“When, as a result of an occurrence that involves a vessel or its equipment, a person dies or disappears from a vessel, the operator shall, without delay, by the quickest means available, notify” relevant Coast Guard reporting authority); 40 CFR 355.40 (immediate reporting of release of hazardous chemicals or substances); 49 CFR 830.5 (requiring operators of private aircraft to “immediately, and by the most expeditious means available, notify” NTSB of an aircraft accident); 49 CFR 171.15 (entitled “Immediate notice of certain hazardous materials incidents” and requiring a telephonic

¹² *See Commonwealth of Massachusetts v. Gagnon et al.*, Case No. 1284CV04568 (Jan. 7, 2013, Suffolk Superior Court) (consent judgment entered against medical offices and their vendor for the disposal of intact medical records containing the personal information of more than 67,000 consumers in a public dump). *See also* <http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-at-dump.html>.

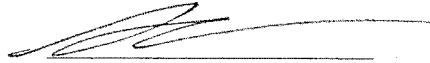
report (within 12 hours) to the National Response Center following a hazardous material incident).

3. *Should the Data Acquisition and Technology Accountability and Security Act give preemption from state laws on breach notification to businesses that do not have to provide notice to consumers or regulators under this bill? If that happens, could it mean that neither state nor federal law requires those businesses to provide notice of a breach to consumers?*

It is our understanding that if an entity did not have to provide notice under the DD or any other federal law, said entity might not be required by either state or federal law to provide notice by operation of the preemption language of section 6. We do not think creating such an enforcement gap is the right approach.

We appreciate this opportunity to provide this additional information to the Committee. In that connection, we seek to reiterate our view of the importance of protecting consumers from data security breaches, including by preserving the States' ability to act swiftly in light of new data security risks. Please do not hesitate to contact us for additional detail or clarity, or with any further questions you may have. Thank you for your consideration.

Sincerely,



Sara Cable
Director of Data Privacy & Security
Assistant Attorney General
Consumer Protection Division
Office of Attorney General Maura Healey
One Ashburton Place
Boston, MA 02108
(617) 727-2200



Consumer Data Industry Association
 1090 Vermont Ave., NW, Suite 200
 Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

May 1, 2018

The Honorable Blaine Luetkemeyer, Chairman
 The Honorable William Lacy Clay, Ranking Member
 Subcommittee on Financial Institutions & Consumer Credit
 Committee on Financial Services
 United States House of Representatives
 Washington, DC 20515

Dear Chairman Luetkemeyer & Ranking Member Clay:

Thank you for the opportunity to appear before your Subcommittee on March 7th to discuss legislative proposals to reform the current data security and breach notification regulatory regime. The hearing was a substantive discussion of an important topic with a wide range of different views represented. The Consumer Data Industry Association appreciates the opportunity to present the views of our members.

On April 12, we received the attached supplemental questions from full-Committee Ranking Member Waters and Representative Ross. I have provided responses to each below.

Question for the Record from Representative Dennis A. Ross

Do you understand the Data Acquisition and Technology Accountability and Security Act to apply exclusively to data stored electronically? Or, would paper files held by covered entities also be subject to the bill's requirements? Are there any concerns with clarifying at the outset that this bill applies only to data stored electronically?

Our understanding is that the bill's provisions would apply to records held in any medium. Given that we believe this is the case, we would have no objection to adding clarifying language to the bill.

Question for the Record from Representative Dennis A. Ross

Under the discussion draft, customer notification is required "immediately" unless it's delayed at the instruction of law enforcement. Can you explain how codifying a specific timeframe may negatively impact customers or an investigation by law enforcement? Do you believe there are standards other than "immediate" that would be better? If so, please explain why. Do you have any other suggestions for how this standard could be improved?

Can you provide me an example of a legal standard requiring "immediate" notification in any other provision of law and explain to me how anyone meets that requirement?

As noted in my written statement, use of the word “immediately” without qualification would suggest that companies would have to disclose the breach before they understood the extent of the breach, made preparations for identity monitoring or other mitigation or closed the vulnerability. Many states require notification “in the most expedient time and manner possible and without unreasonable delay”. While more subjective, this allows breached entities time “to determine the scope of the breach” and the individuals impacted, to restore the “integrity of systems”, and to perform critical security and customer service functions before notification of the breach.

For example, California breach notification law states, “the disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” (See California Civil Code s. 1798.82(a))

While a minority of states require notice within a specific time frame, generally between 30 to 45 days, most states recognize that it is important for a breached entity to conduct an investigation and to complete corrective actions before providing notification. This helps ensure that the security or technological vulnerability has been addressed and the breach notification is provided to the correct consumers and includes the most accurate information regarding the incident.

I am not aware of an unqualified “immediate” standard in law but recognize that one or more may exist. In cases about which I am aware, there are qualifiers around the specific word “immediately” when it appears in law.

Question for the Record from Representative Dennis A. Ross

Should the Data Acquisition and Technology Accountability and Security Act give preemption from state laws on breach notification to businesses that do not have to provide notice to consumers or regulators under this bill? If that happens, could it mean that neither state nor federal law requires those businesses to provide notice of a breach to consumers?

Congress should ensure that a strong, robust, national standard applies across the economy. A breached customer deserves to understand what happened to their information, whether the breach occurred at a credit bureau or at a coffee shop, whether it occurred in Missouri or Maryland. The standard should be flexible and scalable to account for different kinds and sizes of businesses, but it should apply across the nation, to all sectors of the economy.

Question for the Record from Ranking Member Maxine Waters

If Congress adopts the data security DD, which looks to adopt minimum data security and breach notification standards and pre-empt state law, can you comment on why it's important to leave states with the power to continue to innovate and implement consumer protections and data security safeguards?

Can you cite any specific examples where states have taken action to quickly address data security vulnerabilities or gaps in consumer protections that otherwise would have left consumers vulnerable?

We believe that there should be a single, strong national standard to protect consumers and ensure they are notified in a timely fashion should a breach occur. As currently contemplated, the states would retain important functions, particularly in the area of enforcement. I am not aware of instances where states have taken action on data security in the financial services sector prior to a breach to prevent one, but then it would be hard to prove a negative. Instead, we have seen instances where states have been effective enforcers of standards after a breach has occurred.

Question for the Record from Ranking Member Maxine Waters

Consumer Reports has found that "in most cases a credit freeze offers better protections against fraud..." than the credit locks being pushed by the major credit reporting agencies. Nevertheless, Equifax, continues to steer consumers into using its proprietary "lock" product. Can you comment on why Equifax, and other credit reporting agencies are choosing to offer this lock service rather than paying for consumers' security freezes?

A freeze, as defined in state law, is a process where a company and a consumer engage in a transaction to freeze their file, then have no further business relationship until the consumer seeks to "unfreeze" the file. This requires authentication at each interaction, which is a necessarily cumbersome process. The lock product, on the other hand, allows for authentication at the front end, and then an ongoing relationship, removing friction from the system when a consumer seeks to unfreeze the file. However, the impact of the lock and the freeze on the consumer's file is the same: while there is a lock or a freeze in place, a potential creditor cannot access the report to make a firm offer of credit.

Legislation currently being considered by Congress would set a national law for free freezes.

Question for the Record from Ranking Member Maxine Waters

Consumers impacted by the Equifax data breach could find their Experian and TransUnion credit reports affected as well. Given this, what steps are you, as the representative of each of the major credit bureaus doing to ensure that these entities are working together to

ensure comprehensive protections are afforded to consumers across the largest consumer reporting bureaus?

CDIA members conduct business with each other on commercial terms. As their trade association we do not intervene in their commercial relationships as this would conflict with our obligations under antitrust law.

Question for the Record from Ranking Member Maxine Waters

Written testimony by Marc Rotenberg, President of the Electronic Privacy Information Center, succinctly summarized the unique business model of the credit reporting industry, noting that the industry: "Capture[s] the upside value of selling credit reports, and transfer[s] the risk to consumers for breaches and errors." However, in addition to raking in handsome profits from selling credit reports, the industry also capitalizes on consumers' legitimate fears about fraud and identity theft, charging them exorbitant fees for a suite of ID theft monitoring services, lock products, among other services (number formatting below added).

- 1. Of the more than \$9 billion in revenue earned by each of companies-- Equifax, TransUnion, and Experian-- in 2016, what the percentage related, indirectly from any add-on products relating to those products marketed to, and sold by, these companies to consumers as "identify theft" prevention tools or, other iterations of names, such as credit monitoring services or products, and what percentage of these products or services were marketed to, and sold, directly to consumers by these companies?*
- 2. Given that consumers don't have the right to opt out of having consumer reporting agencies collect their sensitive information in the first place, why should they have incur additional, fees, in order to minimize their concerns with the lack of safeguarding of their information? How is the credit reporting industry justify passing on the costs of good corporate governance and cyber security mechanisms to consumers, who already do not receive any explicit financial compensation from these companies use of their data in the first place, Shouldn't this burden be placed on the same companies that are selling this information without even having to obtain consumers' consent?*
- 3. Since the Equifax breach was announced last summer, have consumer reporting agencies that are members of CDIA seen increased revenue from the sale of credit monitoring service or other identity theft prevention products tools like credit or security freezes?*
- 4. Please describe the licensing or other contractual or business organization arrangements that previously, or currently existing, between Equifax, Experian, and TransUnion, over*

the last five years, including a descriptions of third-party providers of credit monitoring or identity theft prevention products, such as Lifelock, with any of these nationwide CRAs or specialty CRAs, and the amount of revenue generated from these business relationships for same time period? In doing so, please list the dollar amount, by quarter, is feasible and, if not deemed practicable, please provide a detailed narrative explaining the legal, statutory and case law preventing its disclosure, and if not able to comply with the quartile requires for information, please provide it to us on annual basis.

1. CDIA members do not each have more than \$9 billion in revenue.

Each of the nationwide CRAs provide services to consumers to enable them to understand and monitor their credit and monitor and help protect their identity. Companies also sell consumer and credit information to resellers who combine credit bureau information with other information to provide additional services for consumers. Due to the 2017 cybersecurity incident, Equifax has ceased advertising for new business as it relates to its US consumer direct business and now provide free services.

According to their SEC filings, total operating revenue for Equifax Global Consumer Solutions was \$402 million in 2016 and \$403 million in 2017. According to their SEC filings, total operating revenue for TransUnion Consumer Interactive was \$407 million in 2016 and \$432 million in 2017. Experian is not an SEC registrant.

2. We believe that it is appropriate for CRAs to be permitted to recover a portion of the costs they incur to operate a state-mandated freeze system. However, legislation currently being considered by Congress would set a national law for free freezes.
3. Revenues at each of the companies rose over the last year, but roughly in line with previous periods. There was no "spike" in revenues as the result of the security incident announced in September.
4. CRAs license other companies to use certain data, software and other technology and intellectual property rights they own and control, on terms that protect their interests in their intellectual property. The companies also buy licenses from other companies to use their data, technology and other intellectual property. For example, companies license credit-scoring algorithms and the right to sell credit scores derived from those algorithms from third parties for a fee.

Beyond publicly available information, CDIA is not privy to additional detailed information regarding commercial relationships between CDIA members. CDIA members conduct business with each other on commercial terms. As their trade

association we do not intervene in their commercial relationships as this would conflict with our obligations under antitrust law.

Question for the Record from Ranking Member Maxine Waters

You recently spoke before Congress at the Subcommittee on Digital Commerce and Consumer Protection, in which you stated, “[C]onsumers today have access to the most democratic and fair credit system ever to exist.” Can you please comment on your vision for CRAs as the “most democratic and fair credit system” in light of today’s discussion along with a supporting empirical research that affirms your provision?

Consumer credit is broadly available based in large part on individual consumers’ past interactions with credit, as expressed by their credit report. It is a meritocratic system that measures people based on their own individual decisions and experience with creditors in past interactions. Consumer credit lending decisions are generally not made based on subjective, impermissible factors such as race, geography or personal connection. This is in contrast to previous periods in our history where lending decisions were made by subjective standards and influenced by such practices as red-lining. Public policy responses such as the Community Reinvestment Act and the Fair Housing Act eliminated many of these practices. Consumer reports – together with the ability to be informed of and challenge disputed information – mean that consumers know what they are being judged on and how. We have the fairest, most transparent and most successful credit reporting system in the world. This is not just CDIA making this point, but the FTC, the Federal Reserve and others.

Then-FTC Chairman Tim Muris referred to the “miracle of instant credit,” whereby a consumer can walk in to an auto dealer and “can borrow \$10,000 or more from a complete stranger, and actually drive away in a new car in an hour or less.” Muris also noted that this

“miracle” is only possible because of our credit reporting system. The system works because, without anybody’s consent, very sensitive information about a person’s credit history is given to the credit reporting agencies. If consent were required, and consumers could decide - on a creditor-by-creditor basis - whether they wanted their information reported, the system would collapse ... The FCRA is an intricate statute that strikes a fine-tuned balance between privacy and the use of consumer information. At its core, it ensures the integrity and accuracy of consumer records and limits the disclosure of such information to entities that have ‘permissible purposes’ to use the information.¹

The Federal Reserve, in a report to Congress, said:

“The available evidence indicates that the introduction of credit-scoring systems has increased the share of applications that are approved for credit, reduced the costs of

¹ FTC Chairman Tim Muris, October 4, 2001 before the Privacy 2001 conference in Cleveland.

underwriting and soliciting new credit, and increased the speed of decisionmaking. It has also made it possible for creditors to readily solicit the business of their competitors.”²

The referenced Board of Governors’ report was submitted to Congress pursuant to §215 of the Fair and Accurate Credit Transactions Act of 2003 and, among other things, studies how the system affects the availability and affordability of credit.

Question for the Record from Ranking Member Maxine Waters

Can you state with percentage can you affirmatively state that there will no more additional American consumers that the public will later be told by Equifax that is has suddenly discovered more harmed consumers have their sensitive and financial institution exposed by an unauthorized data beach? What was date and time in which Equifax inform CDIA about the additional 2.4 million consumes, who also had their personal and sensitive information compromised by bad actors? Did CDIA ask Equifax it as properly informed agencies were informed, and by what method of delivery, about the additional scope of the breach and, if so, what was CDIA told? Did CDI ask Equifax if it had informed its Board Directors of additional harmed consumer and, if not was the inquiry not mad? And, of the question was raised, what date was the entire Board informed of this new finding? Why did it take so long for Equifax, even though it had hired an outside investigative firm, to announce that it had discovered an additional 2.4 million American’s information was involved with the breach last year? Given Equifax’s late discovery of these impacted the consumers, and the statements from witnesses at the “Minority Day” hearing in the Fall, what best practices is CDIA now articulating for its members to conduct an investigation about potential breaches as well as the types of products and services that it should make available to innocent consumers harmed by these companies’ bad practices Can you please provide the Committee with any background information or other material relating to or about “best practices” to prevent a breach, conduct an investigation into it if it is suspected, and how and when it should notify possibly harmed consumers about the breach that it had recommending to its Members before the public announcement of the massive Equifax breach, as well as a copy of any revised, even if not yet finalized, “best practices” from about any of the above mentioned matters?

I cannot state for certain whether there will be more consumers harmed by the Equifax breach. As stated publicly by Equifax, recent announcements are the result of ongoing analysis of data stolen in last year’s cybersecurity incident, and it continues to take broad measures to identify, inform and protect consumers who may have been affected.

I learned of the Equifax breach through the news media late in the afternoon on September 7, 2017. I had no prior knowledge and learned of subsequent information regarding the

² Report to the Congress on Credit Scoring and Its Effects on the Availability and Affordability of Credit, Board of Governors of the Federal Reserve System, Aug. 2007, Pages O-4, 5.

Equifax cybersecurity incident in the same manner. Until the information is released publicly, it is material non-public information, which CDIA is not made aware of in advance.

CDIA is not aware of the specific reason for the timing of Equifax's announcement regarding the additional 2.4 million impacted consumers, other than Equifax's public statement that it was the result of its ongoing analysis of the 2017 cybersecurity incident.

While CDIA does not set standards for member companies' conduct in these matters nor maintain "best practices," we believe that companies should move as quickly as is practicable to inform the public of a breach. This means that a full forensic accounting may not necessarily be complete when information regarding an incident is first publicly announced. As somebody personally impacted by the breach, I would rather the company reported the information as they understood it on September 7th, rather than wait for a full forensic accounting, which could have delayed notification of the incident by months.

Thank you once again for the opportunity to testify at the hearing in March. We look forward to continuing to work with you as you continue to address this important issue.

Sincerely,



Francis Creighton
President & CEO

Attachments: Supplemental questions from Ranking Member Waters
Supplemental questions from Representative Ross

**Questions for Members for the Financial Institutions and Consumer Credit
Subcommittee Hearing Entitled “Legislative Proposals to Reform the Current Data
Security and Breach Notification Regulatory Regime”
Wednesday, March 7, 2018, 2:00 P.M.**

Questions for the entire industry witnesses, except Ms. Sara Cable, who was already submitted as substantially similar question:

- If Congress adopts the data security DD, which looks to adopt minimum data security and breach notification standards and pre-empt state law, can you comment on why it’s important to leave states with the power to continue to innovate and implement consumer protections and data security safeguards?
 - Can you cite any specific examples where states have taken action to quickly address data security vulnerabilities or gaps in consumer protections that otherwise would have left consumers vulnerable?

Questions for Mr. Francis Creighton, President & CEO, Consumer Data Industry Association

Credit Locks & Freezes

- Consumer Reports has found that “In most cases a credit freeze offers better protections against fraud...” than the credit locks being pushed by the major credit reporting agencies. Nevertheless, Equifax, continues to steer consumers into using its proprietary “lock” product. Can you comment on why Equifax, and other credit reporting agencies are choosing to offer this lock service rather than paying for consumers’ security freezes?
- Consumers impacted by the Equifax data breach could find their Experian and TransUnion credit reports affected as well. Given this, what steps are you, as the representative of each of the major credit bureaus doing to ensure that these entities are working together to ensure comprehensive protections are afforded to consumers across the largest consumer reporting bureaus?

Enhancing Public Fear of Identity Theft as a For-fit Business Model for CRAs and Data Brokers

- Written testimony by Marc Rotenberg, President of the Electronic Privacy Information Center, succinctly summarized the unique business model of the credit reporting industry, noting that the industry:

“Capture[s] the upside value of selling credit reports, and transfer[s] the risk to consumers for breaches and errors.” However, in addition to raking in handsome profits from selling credit reports, the industry also capitalizes on consumers’ legitimate fears about fraud and identity theft, charging them exorbitant fees for a suite of ID theft monitoring services, lock products, among other services.

- Of the more than \$9 billion in revenue earned by each of companies-- Equifax, TransUnion, and Experian-- in 2016, what the percentage related, indirectly from any add-on products relating to those products marketed to, and sold by, these companies to consumers as “identify theft” prevention tools or, other iterations of names, such as credit monitoring services or products, and what percentage of these products or services were marketed to, and sold, directly to consumers by these companies?
- Given that consumers don’t have the right to opt out of having consumer reporting agencies collect their sensitive information in the first place, why should they have incur additional, fees, in order to minimize their concerns with the lack of safeguarding of their information? How is the credit reporting industry justify passing on the costs of good corporate governance and cyber security mechanisms to consumers, who already do not receive any explicit financial compensation from these companies use of their data in the first place, Shouldn’t this burden be placed on the same companies that are selling this information without even having to obtain consumers’ consent?
- Since the Equifax breach was announced last summer, have consumer reporting agencies that are members of CDIA seen increased revenue from the sale of credit monitoring service or other identity theft prevention products tools like credit or security freezes?
- Please describe the licensing or other contractual or business organization arrangements that previously, or currently existing, between Equifax, Experian, and TransUnion, over the last five years, including a descriptions of third-party providers of credit monitoring or identity theft prevention products, such as Lifelock,with any of these nationwide CRAs or specialty CRAs,and the amount of revenue generated from these business relationships for same time period? In doing so, please list the dollar amount, by quarter, is feasible and, if not deemed practicable, please provide a detailed narrative explaining the legal, statutory and case law preventing its disclosure, and if not able to comply with the quartile requires for information, please provide it to us on annual basis.

Statement on the fairness of CRAs

- You recently spoke before Congress at the Subcommittee on Digital Commerce and Consumer Protection, in which you stated, “[C]onsumers today have access to the most democratic and fair credit system ever to exist.” Can you please comment on your vision for CRAs as the “most democratic and fair credit system” in light of today’s discussion along with a supporting empirical research that affirms your provision?
- Can you state with percentage can you affirmatively state that there will no more additional American consumers that the public will later be told by Equifax that is has suddenly discovered more harmed consumers have their sensitive and financial institution exposed by an unauthorized data beach? What was date and time in which Equifax inform CDIA about the additional 2.4 million consumes, who also had their personal and sensitive information compromised by bad actors? Did CDIA ask Equifax it as properly informed agencies were informed, and by what method of delivery, about the additional scope of the breach and, if so, what was CDIA told? Did CDI ask Equifax if it had informed its Board Directors of additional harmed consumer and, if not was the inquiry not mad? And, of the question was raised, what date was the entire Board informed of this new finding? Why did it take so long for Equifax, even though it had hired an outside investigative firm, to announce that it had discovered an additional 2.4 million American’s information was involved with the breach last year? Given Equifax’s late discovery of these impacted the consumers, and the statements from witnesses at the “Minority Day” hearing in the Fall, what best practices is CDIA now articulating for its members to conduct an investigation about potential breaches as well as the types of products and services that it should make available to innocent consumers harmed by these companies’ bad practices Can you please provide the Committee with any background information or other material relating to or about “best practices” to prevent a breach, conduct an investigation into it if it is suspected, and how and when it should notify possibly harmed consumers about the breach that it had recommending to its Members before the public announcement of the massive Equifax breach, as well as a copy of any revised, even if not yet finalized, “best practices” from about any of the above mentioned matters?

Questions for the Record

Hearing Title: Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime

Witnesses: Ms. Sara Cable, Mr. Francis Creighton, Mr. John S. Miller, Mr. Jason Kratovil

Member Requesting: Rep. Dennis A. Ross

Question for the Entire Panel

1. Do you understand the *Data Acquisition and Technology Accountability and Security Act* to apply exclusively to data stored electronically? Or, would paper files held by covered entities also be subject to the bill's requirements? Are there any concerns with clarifying at the outset that this bill applies only to data stored electronically?
2. Under the discussion draft, customer notification is required "immediately" unless it's delayed at the instruction of law enforcement. Can you explain how codifying a specific timeframe may negatively impact customers or an investigation by law enforcement? Do you believe there are standards other than "immediate" that would be better? If so, please explain why. Do you have any other suggestions for how this standard could be improved?
 - a. Can you provide me an example of a legal standard requiring "immediate" notification in any other provision of law and explain to me how anyone meets that requirement?

Should the *Data Acquisition and Technology Accountability and Security Act* give preemption from state laws on breach notification to businesses that do not have to provide notice to consumers

May 8, 2018

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions and Consumer Credit
House Committee on Financial Services
Washington, DC 20515

Dear Chairman Luetkemeyer:

Thank you again for the opportunity to testify on March 7, 2018 at your Subcommittee hearing titled "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime." I appreciate the opportunity to respond to the following questions for the record submitted by your colleagues:

Questions from Representative Dennis Ross:

- 1. Do you understand the *Data Acquisition and Technology Accountability and Security Act* to apply exclusively to data stored electronically? Or, would paper files held by covered entities also be subject to the bill's requirements? Are there any concerns with clarifying at the outset that this bill applies only to data stored electronically?**

My understanding is that the author of the Discussion Draft intended the bill to apply to both electronic and paper records. However, that could be made clearer as the draft evolves. While all of the recent headline-grabbing data breaches have involved electronic records, there is no doubt that both paper and electronic records can be compromised.

- 2. Under the discussion draft, customer notification is required "immediately" unless it's delayed at the instruction of law enforcement. Can you explain how codifying a specific timeframe may negatively impact customers or an investigation by law enforcement? Do you believe there are standards other than "immediate" that would be better? If so, please explain why. Do you have any other suggestions for how this standard could be improved?**

The full scope of a breach is rarely clear in the initial phases of an investigation. This is particularly true as it relates to the ability of a breached firm to ascertain with some degree of certainty exactly which of its customers were impacted. Were a federal law to require customer notification in a very short timeframe, I believe it is safe to assume that firms would err on the side of providing notice to a broader universe of customers – likely including individuals not impacted by the breach, potentially causing alarm where none should exist and exacerbating the issue of de-sensitization – since such a narrow legal timeframe would not provide sufficient opportunity to assess the nature and scope of the breach.

As I described in my testimony, FSR believes it is paramount that policymakers approach this question with an eye toward balancing three principles: The vital need for timely notification; a notice that is triggered by an actual risk of harm to customers; and the importance of ensuring the breached entity can get its arms sufficiently around the scope of its breach – not to mention *contain* the breach and restore the integrity of its software and hardware, so that additional consumers are not impacted – so that only the at-risk customers eventually receive notice and are motivated to take action.

Many states and the Gramm-Leach-Bliley Act (GLBA) utilize a threshold for timing based on a concept of “as soon as possible,” with some linguistic variations. A common construction, for example, includes language requiring notice in “the most expeditious time possible and without unreasonable delay.” FSR believes this approach represents the best balance to ensure timely, and accurate, notification.

a. Can you provide me an example of a legal standard requiring “immediate” notification in any other provision of law and explain to me how anyone meets that requirement?

No state data breach notification law requires “immediate” notification to consumers. Of the two federal breach notice standards applicable to specific sectors (HIPAA for healthcare and GLBA for financial services), neither requires “immediate” notification to consumers.

3. Should the *Data Acquisition and Technology Accountability and Security Act* give preemption from state laws on breach notification to businesses that do not have to provide notice to consumers or regulators under this bill? If that happens, could it mean that neither state nor federal law requires those businesses to provide notice of a breach to consumers?

This Discussion Draft aims to create a uniform breach notification standard for all companies, with the exception of those already obligated under existing federal law to provide notice (HIPAA and GLBA, as mentioned previously). Within that breach standard are different requirements for certain entities that are largely dependent on the context through which they came into contact with the personal information. For example, if the personal information was received directly from a consumer, the entity is a “covered entity” under the Draft. If the entity received the personal information from a covered entity for any sort of business purpose through a contractual arrangement, the entity is then a “third party” under the Draft.

The Draft establishes a legal baseline that the covered entity is responsible for providing notice to consumers, even if the breach occurred at a third party to the covered entity. However, it should be noted that the Draft does not prohibit companies from agreeing to different

arrangements via contract (See (c)(2)(A) on page 13 of the Draft), which I believe is a very important clarification. Thus, regardless of where the breach actually took place, the Draft ensures consumers will receive notice.

This construction is found across numerous existing state data breach notification laws. To provide just two examples: Your home state's law (Fla. Stat. §§ 501.171) requires a third party to notify the covered entity of the breach, but then it is the responsibility of the covered entity to provide further notice, including to consumers. Third parties are also required to provide covered entities with "all information that the covered entity needs to comply with its notice requirements," which is similar in concept to the approach in the Draft. Ohio law (Ohio Rev. Code §§ 1349.19), my home state, uses different terminology to refer to "covered entities" and "third parties," but still requires a similar approach: The third party is required to notify the covered entity "in an expeditious manner." Consumer notice responsibility rests with the covered entity.

Whether or not a third party should ever have a statutory obligation to notify consumers is a question that ultimately Congress will need to resolve. Existing state-level precedent that requires the covered entity to provide notice even if the breach occurred at a third party, in my opinion, is based at least in part on the idea that the entity with the closest relationship to the consumer should provide notice because that increases the odds that the consumer will actually pay attention to the notice and take steps to protect themselves. This concept has merit.

Questions from Ranking Member Maxine Waters:

If Congress adopts the data security DD, which looks to adopt minimum data security and breach notification standards and pre-empt state law, can you comment on why it's important to leave states with the power to continue to innovate and implement consumer protections and data security safeguards?

States have certainly earned the moniker "laboratories of democracy" in their leadership on data protection initiatives. However, in my opinion there are few issues that more obviously call for a uniform federal approach than data security and consumer breach notification. As I mentioned in my testimony: Where you live should not determine whether *or if* your personal information is required to be protected.

In my testimony, FSR calls for a strong bill creating a federal standard that preempts existing state laws on both data security and breach notification. The operative word here is "strong," particularly as it relates to data security. Historically, bills in Congress have ranged from having no data protection requirements or a bare-bones requirement that companies should "reasonably" protect data, to extremely detailed requirements that begin to mimic obligations currently imposed on banks. The Discussion Draft strikes a balance that creates a suitably strong standard – one that can actually help prevent data breaches, which in my mind should be the overarching

goal – with flexibility considerations that make it appropriate for the wide range of companies across the U.S. economy.

- **Can you cite any specific examples where states have taken action to quickly address data security vulnerabilities or gaps in consumer protections that otherwise would have left consumers vulnerable?**

Every state – plus D.C., Puerto Rico, the Virgin Islands and Guam – now has a data breach notification law. More than half of the states have laws relating to the disposal and/or destruction of data. At least 13 states have laws specifically requiring the protection of data. These data security laws, much like the federal proposals I described previously, range from requiring “reasonable” policies and procedures, to extremely granular and prescriptive statutes. However, this means that residents in the majority of states in the U.S. live under no data protection requirement, or a fairly minimal standard at best. This is perhaps the single most compelling reason for Congress to enact a preemptive, uniform and strong data security requirement.

Questions for Jason, Vice President of Government Affairs, Financial Services Roundtable

- **The Financial Services Roundtable wrote last November to the Subcommittee calling for the enactment of a national data security and breach notification standard that would eliminate the current inconsistent patchwork of state law. Can you provide at least three specific examples of the inconsistencies that you were referring to in your letter?**
- The State of New York requires notification to consumers “in the most expedient time possible and without unreasonable delay.” The State of Tennessee requires notification to consumers within 45 days.
- Arkansas requires companies to implement and maintain “reasonable security procedures and practices” to secure information. Nevada mandates compliance with the Payment Card Industry (PCI) Data Security Standard. For comparison, the “PCI DSS Quick Reference Guide” alone is a 40-page document.¹
- Massachusetts mandates encryption of personal information. The statute in Oregon lays out a comprehensive framework for the protection of data very similar to the Federal Trade Commissions’ Safeguards Rule; however, it does not mandate specific technologies.

DATA Security Act does not explicitly include Equifax

- **Under the DATA Security DD, the term “covered entity” means any person, partnership, corporation, trust, estate, cooperative, association, or other entity that accesses, maintains, or stores personal, or handles personal information. For purposes of Section 3 of the Act (a section that would direct covered entities to develop “reasonable” security safeguards), a covered entity also includes Federal agencies. However, pursuant to section 5(e) of the Act, this definition for a covered**

¹ Available at: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf

entity effectively does *not* include a financial institution covered under the Gramm-Leach-Bliley Act, including nationwide consumer reporting agencies like Equifax, insurance providers, or health care providers covered under the Health Insurance Portability and Accountability Act (commonly referred to as HITECH Act), which would create disparate breach notification and data security standards for these entities.

- You have expressed your support for this proposal, stating it *“provides a strong standard....and ensures consumers are quickly informed when a breach puts them at risk.”*
- In the wake of the largest credit reporting data security breach that occurred with Equifax, how can Congress reasonably frame this proposal under consideration today, as something beneficial or the consumers when, in fact, the very type of entity breached and one of the main reasons we are here today discussing the topic, arguably it is not covered within this Act. Can you please advise if you believe the intention is to include such entities such as Equifax within the scope of this Act and under what definition do you believe they are covered?

As “non-traditional” participants in financial marketplaces, credit reporting agencies (CRAs) like Equifax are subject to the Federal Trade Commission’s (FTC) authority under the Gramm-Leach-Bliley Act (GLBA) with respect to data security. Under the FTC’s GLBA “Safeguards Rule,” CRAs are required to have measures in place to secure information covered by the GLBA. With respect to data security under the GLBA, the FTC is the regulator and enforcer of the GLBA information security standards with respect to CRAs.

Under the Discussion Draft, CRAs are considered “financial institutions” and thus have the ability to be deemed in compliance if they comply with the information security requirements under GLBA. However, CRAs would be subject to the notification requirements and accompanying enforcement mechanisms under the Draft.

Specifically regarding the Equifax breach, I would suggest the failing was not of the statute (GLBA) but of the company. No law can possibly be written to fully prevent negligence or human error, or stop a nation-state-supported hacker from successfully breaching a company.

Further, as I described in my testimony related to the PROTECT Act, a significant gap exists for CRAs under existing law relative to their lack of oversight and examination to ensure compliance with the information security requirements of GLBA. The PROTECT Act would address this gap, which FSR believes is smart policy.

- **Mr. Kratovil, when Rep. Loudermilk asked if breach notification was mandatory for financial institutions under the Gramm-Leach-Bliley Act (GLBA), even though the language of GLBA does not explicitly require breach notification, you testified that, “They are mandatory. There is nothing about GLBA’s security requirements or notice requirements that are treated as optional.”**

- **In what ways are financial institutions statutorily required to make notice to individuals affected by a breach of security when the text of GLBA is silent as to breach notification and the interpretive guidance issued by banking regulators in 2005 only states that institutions “should” provide breach notice to affected individuals instead of “must” or “shall” provide notice?**

I sincerely appreciate the opportunity to answer this question.

As you know, in 2005, the federal banking agencies jointly issued interagency guidance (interpreting Section 501(b) of GLBA and the Interagency Guidelines) concerning how a financial institution must respond to the unauthorized acquisition or use of customer information. This Guidance is a Safety and Soundness standard issued under the federal banking agencies’ safety and soundness authority under Section 39 of the Federal Deposit Insurance Act, as well as under Section 501(b) of GLBA.

Federal banking agencies examine financial institutions for their compliance with the Guidance. In this regard, the Guidance is not treated as a recommendation: It is a Safety and Soundness standard for which compliance is demanded.

You noted the use of the word “should.” To put that in context: If the financial institution determines misuse of the information “has occurred or is reasonably possible,” the financial institution “should notify the affected customer as soon as possible.” The Guidance uses the term “should” to express a financial institution’s obligation or duty to notify, as opposed to a recommendation. That is, the Guidance requires notice in accordance with its standards, as opposed to only recommending notice.

Furthermore, the Guidance states that financial institutions have “an affirmative duty” to protect customer information from unauthorized access or use. In this regard, the Guidance clarifies that “[n]otifying customers of a security incident involving the unauthorized access or use of the customer’s information in accordance with the standard set forth [in the Guidance] is a key part of that duty.” Again: Notice to customers in accordance with the Guidance is an “affirmative duty.”

Additionally, the Guidance clarifies that “[w]hen customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.”

- **Please provide us with a list of all instances you are aware of in which an enforcement action or fine was brought or levied against a bank or credit union for failure to notify consumers following a data breach.**

The federal banking agencies may fine or otherwise penalize a financial institution for its failure to comply with the Guidance, by – as an example – issuing Matters Requiring Attention (MRAs). As an illustration, in reference to the notification Guidance, the Office of the Comptroller of the Currency (OCC) states: The OCC may treat a bank’s failure to implement the

final guidance as a violation of the Security Guidelines that are enforceable under the procedures set forth in 12 USC 1831p-1, or as an unsafe and unsound practice under 12 USC 1818.

To the best of my knowledge, the most recent enforcement action taken by the OCC was in 2002 against Goleta National Bank for failure to notify its customers of lost loan files.²

- **In 2014, J.P. Morgan Chase suffered a security breach that, by their own account in a Form 8-K filing that fall, affected 83 million account holders, or more individuals than were affected in either the Target or Home Depot breaches that occurred within 12 months of the bank's breach. According to your testimony, breach notification by financial institutions is mandatory and not optional. However, the bank refused to provide notice to affected account holders following its breach, even after it revealed the breach in its filing with the SEC.**
- **How do you reconcile your testimony that financial institutions have a mandatory obligation to notify consumers of their breaches with the facts in this case that show J.P. Morgan Chase refused to notify its own affected account holders? Are you aware of any penalty or fine imposed on J.P. Morgan Chase by banking regulators or other agencies for failing to notify affected individuals of its security breach?**

The GLBA (as implemented through the financial regulators' Interagency Guidance on response programs) requires notice to consumers if a breach of "sensitive customer information" could result in "substantial harm or inconvenience to any customer." The term "sensitive customer information" is defined as "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. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number."³

Based on the company's 8-K filing, the information compromised in the breach was limited to "...[u]ser contact information – name, address, phone number and email address." Further: "[T]here is no evidence that account information for such affected customers – account numbers, passwords, user IDs, dates of birth or Social Security numbers – was compromised during this attack."⁴

Comparing these statements with the thresholds for notification in GLBA suggest that, in my opinion, 1) the circumstances (by virtue of the type of information lost) does not meet the GLBA's "risk of harm" trigger for notification, and 2) the type of information impacted does not meet the GLBA's definition of "sensitive customer information." Thus, as a technical matter,

² Enforcement action available at: <https://www.occ.gov/static/enforcement-actions/ea2002-93.pdf>

³See <https://www.fdic.gov/news/news/financial/2005/fil2705.html>.

⁴ <http://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=1193125-14-362173>

customer notice would not be warranted because this breach presented little or no risk to consumers.

Despite this, it is my understanding that J.P. Morgan Chase did notify its customers, both publicly on its website and through various alerts to impacted customers' digital and mobile accounts.⁵ There was also widespread media coverage of the issue.

As I stated in my testimony, FSR urges policymakers to be very sensitive to the risk that over-notification – by which I mean notifying consumers of a breach when a given breach presents no real risk – leads to desensitization, causing consumers to ignore the notification. This is the opposite outcome policymakers should seek: Consumer notifications *needs to matter*. Consumers should only receive notice when they are legitimately at risk and need to take steps to protect themselves.

Again, thank you for the opportunity to testify and to answer these additional questions from your colleagues.

Sincerely,

/s/

Jason Kratovil
Vice President
Financial Services Roundtable

⁵ See, for example: <https://www.forbes.com/sites/larrymagid/2014/10/02/jp-morgan-chase-warns-customers-about-massive-data-breach/#697a95121e8a>

**Questions for Members for the Financial Institutions and Consumer Credit Subcommittee
Hearing Entitled “Legislative Proposals to Reform the Current Data Security and Breach
Notification Regulatory Regime”
Wednesday, March 7, 2018, 2:00 P.M.**

Questions for the entire industry witnesses, except Ms. Sara Cable, who was already submitted as substantially similar question:

- **If Congress adopts the data security DD, which looks to adopt minimum data security and breach notification standards and pre-empt state law, can you comment on why it’s important to leave states with the power to continue to innovate and implement consumer protections and data security safeguards?**

ITI Response: There are currently 54 different breach notification regimes in 50 states and four U.S. territories. While there is no vacuum of consumer protection under this patchwork – consumers across the country have for years received notifications pursuant to these laws – the scope of legal obligations following a data breach is broad and complex because each of these notification laws varies by some degree, and some directly conflict with one another. 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 respect to data security safeguards, today there is an expanding, convoluted patchwork of state data security laws, with more than a dozen states imposing laws regulating how data must be secured, including Arkansas, California, Connecticut, Florida, Indiana, Kansas, Maryland, Massachusetts, Minnesota, Nevada, New Mexico, Oregon, Rhode Island, Texas, and Utah. These data security safeguards vary wildly from state to state, ranging from requiring reasonable procedures appropriate to the sensitivity of the data, to more prescriptive, compliance-based “check the box” approaches. Federal data breach notification legislation not only offers the opportunity to streamline the notification requirements into a single, uniform procedure, but to enhance the security landscape by incentivizing the adoption of security principles by entities in all 50 states that are flexible, risk-based, remain “evergreen,” and are adaptable to ever-changing threats. The federal government should seize its opportunity to innovate data security safeguards, and raise all boats to a common security standard.

- **Can you cite any specific examples where states have taken action to quickly address data security vulnerabilities or gaps in consumer protections that otherwise would have left consumers vulnerable?**

ITI Response: While I cannot cite a specific example of where a state has acted “quickly” to address data security vulnerabilities, to a certain extent I am sure any of the dozen-plus states that have adopted data security safeguards as part of their data breach laws can be said to have helped ensure minimum data security standards. As Ms. Cable pointed out in her testimony, Massachusetts has been a leader in imposing such security safeguards. If Congress passes a law that adopts security principles that are flexible, risk-based, remain “evergreen,” and are adaptable to ever-changing threats, there will not be a need for states to “innovate” further security safeguards.

Questions for Mr. Francis Creighton, President & CEO, Consumer Data Industry Association

Credit Locks & Freezes

- Consumer Reports has found that “In most cases a credit freeze offers better protections against fraud...” than the credit locks being pushed by the major credit reporting agencies. Nevertheless, Equifax, continues to steer consumers into using its proprietary “lock” product. Can you comment on why Equifax, and other credit reporting agencies are choosing to offer this lock service rather than paying for consumers’ security freezes?
- Consumers impacted by the Equifax data breach could find their Experian and TransUnion credit reports affected as well. Given this, what steps are you, as the representative of each of the major credit bureaus doing to ensure that these entities are working together to ensure comprehensive protections are afforded to consumers across the largest consumer reporting bureaus?

Enhancing Public Fear of Identity Theft as a For-fit Business Model for CRAs and Data Brokers

- Written testimony by Marc Rotenberg, President of the Electronic Privacy Information Center, succinctly summarized the unique business model of the credit reporting industry, noting that the industry:
 - “Capture[s] the upside value of selling credit reports, and transfer[s] the risk to consumers for breaches and errors.” However, in addition to raking in handsome profits from selling credit reports, the industry also capitalizes on consumers’ legitimate fears about fraud and identity theft, charging them exorbitant fees for a suite of ID theft monitoring services, lock products, among other services.
 - Of the more than \$9 billion in revenue earned by each of companies-- Equifax, TransUnion, and Experian-- in 2016, what the percentage related, indirectly from any add-on products relating to those products marketed to, and sold by, these companies to consumers as “identify theft” prevention tools or, other iterations of names, such as credit monitoring services or products, and what percentage of

these products or services were marketed to, and sold, directly to consumers by these companies?

- Given that consumers don't have the right to opt out of having consumer reporting agencies collect their sensitive information in the first place, why should they have incur additional, fees, in order to minimize their concerns with the lack of safeguarding of their information? How is the credit reporting industry justify passing on the costs of good corporate governance and cyber security mechanisms to consumers, who already do not receive any explicit financial compensation from these companies use of their data in the first place, Shouldn't this burden be placed on the same companies that are selling this information without even having to obtain consumers' consent?
- Since the Equifax breach was announced last summer, have consumer reporting agencies that are members of CDIA seen increased revenue from the sale of credit monitoring service or other identity theft prevention products tools like credit or security freezes?
- Please describe the licensing or other contractual or business organization arrangements that previously, or currently existing, between Equifax, Experian, and TransUnion, over the last five years, including a descriptions of third-party providers of credit monitoring or identity theft prevention products, such as Lifelock, with any of these nationwide CRAs or specialty CRAs, and the amount of revenue generated from these business relationships for same time period? In doing so, please list the dollar amount, by quarter, is feasible and, if not deemed practicable, please provide a detailed narrative explaining the legal, statutory and case law preventing its disclosure, and if not able to comply with the quartile requires for information, please provide it to us on annual basis.

Statement on the fairness of CRAs

- You recently spoke before Congress at the Subcommittee on Digital Commerce and Consumer Protection, in which you stated, “[C]onsumers today have access to the most democratic and fair credit system ever to exist.” Can you please comment on your vision for CRAs as the “most democratic and fair credit system” in light of today’s discussion along with a supporting empirical research that affirms your provision?
- Can you state with percentage can you affirmatively state that there will no more additional American consumers that the public will later be told by Equifax that is has suddenly discovered more harmed consumers have their sensitive and financial institution exposed by an unauthorized data beach? What was date and time in which Equifax inform CDIA about the additional 2.4 million consumes, who also had their personal and sensitive information compromised by bad actors? Did CDIA ask Equifax it as properly informed agencies were informed, and by what method of delivery, about the additional scope of the breach and, if so, what was CDIA told? Did CDI ask Equifax if it had informed its Board Directors of additional harmed consumer and, if not was the inquiry

not mad? And, of the question was raised, what date was the entire Board informed of this new finding? Why did it take so long for Equifax, even though it had hired an outside investigative firm, to announce that it had discovered an additional 2.4 million American's information was involved with the breach last year? Given Equifax's late discovery of these impacted the consumers, and the statements from witnesses at the "Minority Day" hearing in the Fall, what best practices is CDIA now articulating for its members to conduct an investigation about potential breaches as well as the types of products and services that it should make available to innocent consumers harmed by these companies' bad practices. Can you please provide the Committee with any background information or other material relating to or about "best practices" to prevent a breach, conduct an investigation into it if it is suspected, and how and when it should notify possibly harmed consumers about the breach that it had recommending to its Members before the public announcement of the massive Equifax breach, as well as a copy of any revised, even if not yet finalized, "best practices" from about any of the above mentioned matters?

**Questions for Members for the Financial Institutions and Consumer Credit Subcommittee
Hearing Entitled “Legislative Proposals to Reform the Current Data Security and Breach
Notification Regulatory Regime”
Wednesday, March 7, 2018, 2:00 P.M.**

Questions for Jason, Vice President of Government Affairs, Financial Services Roundtable

- The Financial Services Roundtable wrote last November to the Subcommittee calling for the enactment of a national data security and breach notification standard that would eliminate the current inconsistent patchwork of state law. Can you provide at least three specific examples of the inconsistencies that you were referring to in your letter?

DATA Security Act does not explicitly include Equifax

- Under the DATA Security DD, the term “covered entity” means any person, partnership, corporation, trust, estate, cooperative, association, or other entity that accesses, maintains, or stores personal, or handles personal information. For purposes of Section 3 of the Act (a section that would direct covered entities to develop “reasonable” security safeguards), a covered entity also includes Federal agencies. **However, pursuant to section 5(e) of the Act, this definition for a covered entity effectively does not include a financial institution covered under the Gramm-Leach-Bliley Act, including nationwide consumer reporting agencies like Equifax,** insurance providers, or health care providers covered under the Health Insurance Portability and Accountability Act (commonly referred to as HITECH Act), which would create disparate breach notification and data security standards for these entities.
 - You have expressed your support for this proposal, stating it “provides a strong standard....and ensures consumers are quickly informed when a breach puts them at risk.”
 - In the wake of the largest credit reporting data security breach that occurred with Equifax, how can Congress reasonably frame this proposal under consideration today, as something beneficial or the consumers when, in fact, the very type of entity breached and one of the main reasons we are here today discussing the topic, arguably it is not covered within this Act. **Can you please advise if you believe the intention is to include such entities such as Equifax within the scope of this Act and under what definition do you believe they are covered?**
- Mr. Kratovil, when Rep. Loudermilk asked if breach notification was mandatory for financial institutions under the Gramm-Leach-Bliley Act (GLBA), even though the language of GLBA does not explicitly require breach notification, you testified that, “They are mandatory. There is nothing about GLBA’s security requirements or notice requirements that are treated as optional.”
- In what ways are financial institutions statutorily required to make notice to individuals affected by a breach of security when the text of GLBA is silent as to breach notification and the interpretive guidance issued by banking regulators in 2005 only states that institutions “should” provide breach notice to affected individuals instead of “must” or “shall” provide notice?

- Please provide us with a list of all instances you are aware of in which an enforcement action or fine was brought or levied against a bank or credit union for failure to notify consumers following a data breach.
- In 2014, J.P. Morgan Chase suffered a security breach that, by their own account in a Form 8-K filing that fall, affected 83 million account holders, or more individuals than were affected in either the Target or Home Depot breaches that occurred within 12 months of the bank's breach. According to your testimony, breach notification by financial institutions is mandatory and not optional. However, the bank refused to provide notice to affected account holders following its breach, even after it revealed the breach in its filing with the SEC.
- How do you reconcile your testimony that financial institutions have a mandatory obligation to notify consumers of their breaches with the facts in this case that show J.P. Morgan Chase refused to notify its own affected account holders? Are you aware of any penalty or fine imposed on J.P. Morgan Chase by banking regulators or other agencies for failing to notify affected individuals of its security breach?

**Questions for Members for the Financial Institutions and Consumer Credit Subcommittee
Hearing Entitled “Legislative Proposals to Reform the Current Data Security and Breach
Notification Regulatory Regime”
Wednesday, March 7, 2018, 2:00 P.M.**

**Questions for Mr. John Miller, Vice President for Global Policy and Law, Information
Technology Industry Council**

Early Notification outweighs potential vulnerability

- In your testimony, you highlight your concerns with the “immediate” notification requirement, stating, “the timeline for notification should reflect the realities of completing an investigation and putting in place the apparatus necessary to notify very large numbers of consumers....immediate notification is not only infeasible, it constitutes a bad security practice that puts consumers at risk of further harm, if notification is required before vulnerabilities have been rectified.”
 - Based on your testimony, can you please comment, in more detail, on why you believe “immediate” notification to consumers of potential breaches of their most personal information, does not in any circumstance outweigh completed preliminary investigations, and where subsequent investigations may take months before individuals who could of taken action, i.e. credit freezes, may become aware and at which point may be made worse?

ITI Response: The primary risk relates to the situation where the vulnerability that resulted in the breach of security has not been remediated. If a covered entity notifies the public that a breach has occurred before the “hole” has been “patched,” the covered entity is essentially painting a target on the backs of consumers, by inviting additional criminal actors to help themselves to the vulnerable personal information exposed by the breach. In this scenario, consumers who have already been victimized by the first criminal actor may now be victimized by follow-on criminal actors, and consumers who were lucky enough to not be victimized by the first criminal actor are at risk of being victimized by the follow-on criminal actors. Notifying consumers that a breach has occurred under such circumstances is simply a bad security practice.

Third party standard viewed as to weak

- You have highlighted your concerns with the standard proposed by the DATA Security DD, in particular the language under Section 4(c)(1), which would require third parties to notify covered entities whose data, “*has or may have been compromised.*” You propose that this clause should be amended to instead state that, “*has been compromised.*” This vital change would make it the only trigger action by a third party when there is “hard evidence that indicates that a compromise in fact occurred and resulted in exfiltration of the covered entities data.”

- o Can you please comment, if entities such as Equifax, are potentially to be interpreted as third parties, how would your amended standard of helping performed by the covered entities to ensure the best way to meet consumers' interests and adequately protect them, are focused on during the revelations of the breach?

ITI Response: ITI's data breach notification policy positions begin with the premise that a data breach notification bill is intended chiefly to achieve greater consumer protection. If third parties are not allowed the time and opportunity to properly determine whether a breach actually occurred, the discussion draft would trigger a wave of notices that (a) notify and unnecessarily alarm consumers if the investigation reveals no actual breach or breach that triggers the statutory risk threshold occurs; and (b) results in "notice fatigue," whereby consumers ultimately ignore the notifications because they are ultimately proven to be false positives. ITI's recommendation is to mirror the procedures afforded to covered entities under Section 4(a), under which a covered entity who believes a breach of security occurred is permitted to investigate to assess the nature and scope of the incident (Section 4(a)(1)), identify whether personal information was impacted (Section 4(a)(2)), determine whether the personal information was acquired without authorization (Section 4(a)(3)), and afforded time to remediate the vulnerability so as to not places consumers at further risk of harm (Section 4(a)(4)).

Questions for the Record

Hearing Title: Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime

Witnesses: Ms. Sara Cable, Mr. Francis Creighton, Mr. John S. Miller, Mr. Jason Kratovil

Member Requesting: Rep. Dennis A. Ross

Question for the Entire Panel

1. Do you understand the *Data Acquisition and Technology Accountability and Security Act* to apply exclusively to data stored electronically? Or, would paper files held by covered entities also be subject to the bill's requirements? Are there any concerns with clarifying at the outset that this bill applies only to data stored electronically?

ITI Response: Section 3(a) of the discussion draft appears to require all records to be safeguarded, regardless of whether the data is in electronic or paper form. If a first party experiences a breach of data security wherein the risk threshold is met under Section 4(b)(2), the first party must notify consumers regardless of whether the breached data is in electronic or paper form. However, the Requirements of Third Parties (Section 4(c)) and Requirements of Service Providers (Section 4(d)) are limited to breaches of data stored electronically. While ITI does not have strong concerns with clarifying that the bill applies only to data stored electronically, particularly if the goal is to align the requirements imposed on first parties and third parties, we do note that doing so would create a gap in coverage. ITI's preference would be that personal information in all forms should be afforded equal protection, whether stored electronically or in other formats.

2. Under the discussion draft, customer notification is required "immediately" unless it's delayed at the instruction of law enforcement. Can you explain how codifying a specific timeframe may negatively impact customers or an investigation by law enforcement? Do you believe there are standards other than "immediate" that would be better? If so, please explain why. Do you have any other suggestions for how this standard could be improved?

ITI Response: If vulnerabilities are not remediated before notification is triggered, consumers will be subject to further harm by would-be thieves who are alerted to the vulnerabilities by public notice. The discussion draft must allow companies to restore the reasonable integrity, security, and confidentiality of the data system before notifying consumers – otherwise, they are effectively painting targets on consumers' backs. Further, law enforcement must be permitted adequate time to perform the complex forensic investigation necessary to identify the criminal hacker or hackers without putting the criminals on notice that investigators are on their trail. Notifying criminals that law enforcement is on their trail would enable the criminals to erase their digital tracks and stymie the investigation. The complexity of investigations, and therefore the time

required, will undoubtedly vary based on whether the criminal is a nation state, a sophisticated and geographically diverse band, or individual.

The timeline for notification should reflect the realities of completing an investigation and putting in place the apparatus necessary to notify very large numbers of consumers. Unfortunately, the timeframe in the discussion draft combines the two competing concepts of “immediately...and without unreasonable delay,” resulting in a mandate that is confusing and counterproductive. We recognize the urgency required for notification and recommend utilizing language from one of the existing state laws to convey such urgency. For instance, both New York and California require consumer notification “in the most expedient time possible and without unreasonable delay.”

- a. Can you provide me an example of a legal standard requiring “immediate” notification in any other provision of law and explain to me how anyone meets that requirement?

ITI Response: First, when discussing breach notification time periods, it is important to differentiate the parties to whom the requirements are requiring notification. While the laws of the states may change frequently and quickly, I am unaware of any requirements in data breach notification laws that require “immediate” notification to consumers or regulators. While some states do require third parties maintaining and/or storing (but not owning) computerized data that includes personal information to notify the owner or licensee of that data of any security breach “immediately” following discovery of such security breach, ITI does not believe it is practicable or advisable to require companies to comply with an “immediate” notification requirement, for the reasons stated previously. A better approach is that taken by Massachusetts, which requires a person that maintains or stores but does not own or license data that includes personal information about a Massachusetts resident to provide notice of a security breach to the owner or licensor of the data “as soon as practicable and without unreasonable delay.”

3. Should the *Data Acquisition and Technology Accountability and Security Act* give preemption from state laws on breach notification to businesses that do not have to provide notice to consumers or regulators under this bill? If that happens, could it mean that neither state nor federal law requires those businesses to provide notice of a breach to consumers?

ITI Response: Yes, the bill should grant preemption for third parties. The bill requires third parties to notify the covered entity – with whom the third party has the direct relationship and who is the owner or licensor of the data – of the breach of security, who will then ultimately notify the consumer with whom they have the direct relationship. However, when the same party is considered a covered entity under the bill – meaning

they are the owner or licensor of the data themselves -- they are required by the discussion draft to notify consumers and regulators. In either event, under the discussion draft consumers will ultimately be notified if the risk threshold is met. Provided the risk threshold of the discussion draft is met, there is no scenario where consumers will not be notified of a known breach of security suffered by a third party.

Questions for the Record

Hearing Title: Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime

Witness: Mr. John S. Miller

Member Requesting: Rep. Dennis A. Ross

1. Mr. Miller, in a response to a question on third-party breach notification requirements from Chairman Luetkemeyer, you testified that, "The entities with whom the consumers have a relationship should be the ones providing that sort of notice." In the case of a data breach regarding credit card information, consumers have a relationship with the financial institution that issued the card to them and bills them monthly for it at the consumer's known address. A business, particularly a store, that accepts a card for payment of goods or services, for example, typically does not have the billing contact information for a cardholder and typically has nothing more than the number and a name. In a situation where a third party, such as a cloud service provider or a payment card processor suffers a breach of security affecting a payment card number alone (a type of covered information in the bill), is it your view that the card-issuing financial institution or the store in which the card was swiped or inserted should have the responsibility to provide notification to affected consumers?

ITI Response: ITI's data breach notification policy positions begin with the premise that a data breach notification bill is intended chiefly to achieve greater consumer protection. A consumer is most likely to open and read a letter or electronic notice if they recognize the name of the sender as someone with whom they have a relationship and trust that the sender is sharing valuable and important information. In reality, many organizations contract with third parties to maintain or process data containing personal information, and given that consumers may be unaware of these third-party relationships 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, and the consumer-facing company and the third party should have the flexibility to determine (via contracts, for instance) which entity should notify consumers.

Additionally, do you believe the third-party cannot make this notice because it may lack the contact information and, in that case, how is it any different than the store that lacks the same information?

ITI Response: In many cases a third party will not hold consumer contact information, which will complicate notification. However, in any data breach involving consumers, there will of course always be a consumer-facing company. The consumer-facing company and any third party service providers with whom that company does business should have the flexibility to determine (e.g., via contracts) which entity should have the responsibility to notify consumers in the case of a breach. ITI does not have a position on whether, generally speaking, a store versus a bank should notify the consumer in the event of a breach of security – the parties should be free to determine that responsibility amongst themselves.

2. Mr. Miller, in your response to Rep. Rothfus' question regarding how to tailor data security obligations for companies of different sizes and in different industries, you said that small companies that don't hold personal or sensitive financial information should not have the same data security obligations as larger nationwide companies or financial institutions. If a breach occurs in the payment process, doesn't that mean that the small retail shop which does not have contact information should not be expected to provide notice to an affected customer? In this scenario, shouldn't the financial institutions that issued the cards to the cardholders and has billing contact information be the one to provide notice of the breach, especially if it was not the small store itself that suffered the breach?