SECURING CONSUMERS' CREDIT DATA IN THE AGE OF DIGITAL COMMERCE

HEARING

BEFORE THE

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

NOVEMBER 1, 2017

Serial No. 115–70

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

U.S. GOVERNMENT PUBLISHING OFFICE
27–917 PDF WASHINGTON : 2018

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon
Chairman

JOE BARTON, Texas
Vice Chairman
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
TIM WALBERG, Michigan
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

ROBERT E. LATTA, Ohio
Chairman

GREGG HARPER, Mississippi
Vice Chairman
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
DAVID B. MCKINLEY, West Virgina
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
LARRY BUCSHON, Indiana
MARKWAYNE MULLIN, Oklahoma
MIMI WALTERS, California
RYAN A. COSTELLO, Pennsylvania
GREG WALDEN, Oregon *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
BEN RAY LUJÁN, New Mexico
YVETTE D. CLARKE, New York
TONY CÁRDENAS, California
DEBBIE DINGELL, Michigan
DORIS O. MATSUI, California
PETER WELCH, Vermont
JOSEPH P. KENNEDY, III, Massachusetts
GENE GREEN, Texas
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

WITNESSES

SUBMITTED MATERIAL

[1] Mr. Schneier did not answer submitted questions for the record by the time of printing.

SECURING CONSUMERS' CREDIT DATA IN THE AGE OF DIGITAL COMMERCE

WEDNESDAY, NOVEMBER 1, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:32 a.m. in Room 2123, Rayburn House Office Building, Hon. Robert E. Latta (chairman of the subcommittee) presiding.

Members present: Representatives Latta, Harper, Burgess, Lance, Guthrie, McKinley, Kinzinger, Bilirakis, Bucshon, Mullin, Walters, Costello, Walden (ex officio), Schakowsky, Cárdenas, Dingell, Matsui, Welch, Kennedy, Green, and Pallone (ex officio).

Also present: Representatives Barton, Cramer, and Duncan.

Staff present: Kelly Collins, Staff Assistant; Zack Dareshori, Staff Assistant; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations/Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Katie McKeogh, Press Assistant and Digital Coordinator; Alex Miller, Video Production Aide and Press Assistant; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Everett Winnick, Director of Information Technology; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Jeff Carroll, Minority Staff Director; Lisa Goldman, Minority Counsel; Caroline Paris-Behr, Minority Policy Analyst; Tim Robinson, Minority Chief Counsel; and C.J. Young, Minority Press Secretary.

Mr. LATTA. Well, good morning. I would like to call the Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection to order. And I also wanted to thank our witnesses for being here this morning. And I recognize myself for a 5-minute opening statement.

OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

One month ago, this subcommittee was the first to hear testimony from former Equifax CEO Richard Smith about how his company's failure to protect against a known security data vulner-

ability led to the exposure of over 145 million Americans' sensitive information.

Today, we continue our investigation into the Equifax breach. We will focus on: helping the public get answers; how is the industry responding to this breach; what the industry response has been to this breach; has the cybersecurity landscape changed as a result of the breach; and what laws and regulations govern the protection of individuals' information collected by businesses.

On Friday, our full committee chairman, Greg Walden, raised questions about how the actions taken by businesses that use personal data affect security, privacy, and individuals' online identities. The Equifax data breach was a stark demonstration of the responsibility that credit bureaus and all companies have when holding millions of Americans' sensitive information. In fact, Congress has recognized the sensitivity of this data and specifically enacted laws regarding the credit bureaus' business model.

Today, we are looking for answers about how best to secure consumers' credit data in order to protect against another breach of this magnitude. We want to shine a light on security practices and understand a path forward to restore confidence to U.S. consumers.

For example, lenders, including banks and retailers, use credit reports and related data to evaluate the likelihood that borrowers will repay their loans. This credit information assists consumers in accessing credit, buying a house, or securing a job. However, consumers may not know or understand what data has been collected on them and how it is being used by the credit reporting industry and their paying customers, including the Federal Government. Today, we hope to shed light on these questions and provide more information for those consumers.

With regard to Equifax, the subcommittee has taken a comprehensive review of the circumstances surrounding the breach. For example, it came to our attention last month that the Internal Revenue Service had awarded a no-bid contract to Equifax. On October 10, Ranking Member Schakowsky and I, along with Chairman Walden and Ranking Member Pallone, sent a bipartisan letter to the IRS Commissioner raising questions about the IRS decision to award a contract to Equifax for identity verification services in the aftermath of the Equifax breach. That contract has since been rescinded.

We also sent a bipartisan letter on October 16 to the General Services Administration about the agency's consideration of data security practices when vetting vendors, like Equifax, and awarding Government contracts. We are looking forward to the GSA's response.

Chairman Walden and I remain committed to working in a bipartisan fashion to get answers for the American public and to hold Equifax accountable.

When former CEO Richard Smith came to Washington last month, he said, quote, "The breach occurred because of both human error and technology failures." These quote/unquote "errors" and "failures" allowed criminals to access over 145 million Americans' data. As a result, names, addresses, birth dates, and full nine-digit Social Security numbers were exposed and certain drivers licenses, credit cards, and credit dispute information were taken.

If your credit card information is stolen, you can contact Visa or MasterCard, and they will reissue a new card and a credit card number. If your Social Security number is stolen, it is much, much more complicated to get a new number. A Social Security number is intrinsically tied to each and every one of us.

According to the FTC, there were nearly 400,000 identity-theft complaints in 2016, which amounts to 13 percent of all consumer complaints received. Nearly 30 percent of consumers reported that their data was used to commit tax fraud in 2016. Consumers also reported that their stolen data was used for credit card fraud, rising to more than 32 percent in 2016 from nearly 16 percent in 2015.

In the aftermath of the Equifax breach, months later, consumers may still be confused about how best to protect themselves. This subcommittee and agencies like the Federal Trade Commission have been providing useful information to consumers in the aftermath of the Equifax breach, but the post-breach consumer protection responses from Equifax have yet to be reassuring.

Data collected and stored by credit bureaus must be protected and safeguarded at all times, and when a breach happens, consumers need swift and concrete answers from the company affected. There are important questions about the best ways to protect sensitive data, including cybersecurity standards, trends, best practices, and emerging threats, particularly with respect to known cybersecurity vulnerabilities.

There are also important questions about the regulatory landscape in which the credit bureaus operated before this massive breach, especially the legal and regulatory framework for credit bureaus, including the safeguards framework in the Gramm-Leach-Bliley Act and consumer protections contained in the Fair Credit Reporting Act.

Also, what is the relationship between data breaches and the incidence of identity theft and fraud? Data breaches may have become so commonplace that data experts and security experts have expressed concerns about breach fatigue.

Congress cannot afford to be lax or idle in its oversight of these critical issues. The testimony today is an important step toward answering the many questions that consumers are looking for, and I look forward to hearing from our witnesses today.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

One month ago, this subcommittee was the first to hear testimony from former Equifax CEO Richard Smith about how his company's failure to protect against a known data security vulnerability led to the loss of over 145 million Americans' sensitive information.

Our investigation continues into the Equifax breach and today's hearing is another step to get answers for the public about:

- what the industry response has been to this breach,
- if the cybersecurity landscape has shifted as a result of the breach, and
- what laws and regulations are at issue.

On Friday, our Full Committee Chairman Greg Walden authored an op-ed in which he raised questions about how actions taken by businesses built around individual's data affect security, privacy, and individual's online identities. All of these issues are critically important to understand in our digital economy and I look for-

ward to working with the chairman and my fellow subcommittee chairman on these issues in the coming months.

The Equifax data breach was a stark demonstration of the responsibility that credit bureaus and all companies have when holding millions of Americans' sensitive information. In fact, Congress has recognized the sensitivity of this data and specifically enacted laws regarding the credit bureau business model.

Today, we are looking for answers about how best to secure consumers' credit data in order to protect against another breach of this magnitude.

We want to shine a light on security practices and understand the path forward to restore confidence to U.S. consumers.

Credit bureaus prepare credit reports based upon individuals' financial transactions history to provide such reports to third parties.

For example, lenders, including banks and retailers, use credit reports and related data to evaluate the likelihood that borrowers will repay their loans.

This credit information assists consumers in accessing credit, buying a house, or securing a job.

However, consumers may not know or understand what data has been collected on them and how it's being used by the credit reporting industry and their paying customers, including the Federal Government.

The subcommittee has taken a comprehensive review of the circumstances around the breach.

For example, it came to our attention last month that the Internal Revenue Service had awarded a no-bid contract to Equifax.

On October 10th, Ranking Member Schakowsky and I, along with Chairman Walden and Ranking Member Pallone, sent a bipartisan letter to IRS Commissioner John Koskinen raising concerns about the IRS's decision to award a contract to Equifax for identity verification services in the aftermath of the Equifax breach. The contract has since been rescinded.

We also sent a bipartisan letter on October 16th to the General Services Administration about the agency's consideration of data security practices when vetting vendors like Equifax and awarding Government contracts. We look forward to GSA's response.

I thank my colleagues across the aisle for working together on this serious matter. Chairman Walden and I remain committed to working in a bipartisan fashion to get answers for the American public and to hold Equifax accountable.

When former CEO Richard Smith came to Washington last month, he said quote: "the breach occurred because of both human error and technology failures."

These quote-unquote "errors" and "failures" allowed criminals to access over 145 million Americans' data.

As a result, names, addresses, birthdates, and full nine-digit Social Security numbers were exposed.

And certain driver's license, credit card, and credit dispute information were taken.

If your credit card information is stolen, you can contact Visa or MasterCard and they'll reissue you a new card and credit card number.

If your Social Security number is stolen, it's much, much more complicated to get a new number.

A Social Security number is intrinsically tied to each and every one of us.

According to the FTC, there were nearly 400,000 identity theft complaints in 2016, or 13 percent of all consumer complaints received, with 29 percent of consumers reporting that their data was used to commit tax fraud in 2016.

Consumers also reported that their stolen data was used for credit card fraud; rising to more than 32 percent in 2016 from nearly 16 percent in 2015.

In the aftermath of the Equifax breach, months later, consumers may still be confused about how best to protect themselves.

All of this is disconcerting, and frankly unacceptable.

This subcommittee, and agencies like the Federal Trade Commission, have been providing useful information to consumers in the aftermath of the Equifax breach.

But the post-breach consumer protection responses from Equifax have yet to be reassuring.

Data collected and stored by credit bureaus must be protected and safeguarded at all times, and when a breach happens consumers need swift and concrete answers from the company affected.

Our subcommittee members continue to ask whether consumers can be confident in the security of their data.

There are important questions about the best ways to protect sensitive data, including cybersecurity standards, trends, best practices and emerging threats particularly with respect to known cybersecurity vulnerabilities.

There are also important questions about the regulatory landscape in which the credit bureaus operated before this massive breach.

For example, what is the legal and regulatory framework for credit bureaus, including the safeguards framework in the Gramm-Leach-Bliley Act and consumer protections contained in the Fair Credit Reporting Act?

Finally, what is the relationship between data breaches and incidence of identity theft and fraud?

Data breaches may have become so commonplace that data security experts have expressed concerns about "breach fatigue."

Though there may be fatigue, Congress cannot afford to be lax or idle in its oversight over these critical issues.

I look forward to the testimony of the panel.

Mr. LATTA. And the Chair now recognizes the ranking member of the subcommittee from Illinois for 5 minutes. The gentlelady is recognized.

Ms. SCHAKOWSKY. I thank you, Mr. Chairman.

Before I give my opening remarks, I must mention that I actually considered raising a point of order against the subcommittee accepting testimony from James Norton at the hearing today.

I want to make perfectly clear that I am not objecting to anything that Mr. Norton might say, but this committee has rules of order, and they need to be followed. James Norton was not listed on the memorandum that was distributed by the committee, and we found out that he was going to testify last night and saw testimony very late last night.

While I understand that another witness was unable to make the hearing today because of illness, this last-minute replacement is really not respectful to the members of the subcommittee. It is disrespectful to the other witnesses on the panel. It is disrespectful, I believe, to the millions of Americans that are concerned about the security of their credit information. And it violates the committee's rules.

So Mr. Norton is here and ready to testify, and I appreciate that he was able to prepare so quickly. I will not be objecting today, but I do want to make it clear that violations of the committee rules are not acceptable and that I will object if this happens again.

I want to also say that I appreciate the bipartisan way in which we have been able to work together. The rules are important.

So if I could begin——

Mr. LATTA. Thank you very much. And the lady is recognized for 5 minutes. Thank you.

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

Ms. SCHAKOWSKY. Thank you.

So today we continue our conversation on data security in the wake of the Equifax data breach.

In our October 3rd hearing with former Equifax CEO Richard Smith, I asked him if I, as a consumer, can opt out of Equifax. After all, I never opted in. Equifax collects my data—that is, like, 1,500 pieces of information on each individual—whether I want it to or not, and now my data is at risk because Equifax failed to adequately protect it.

Mr. Smith essentially said, "No, you can't opt out. That's not how it works." This is incredibly frustrating for consumers, including

the 145.5 million victims of the Equifax breach. That is about half the population. We have little power to protect their sensitive personal information, as credit reporting agencies and data brokers go under-regulated and under-scrutinized. I venture to say a lot of people didn't even know about Equifax until the breach came out.

We need to change that power balance by strengthening consumer protections around credit data. I don't buy the narrative that the Equifax breach happened because of a single careless employee. The system in place at Equifax allowed for a known and well-publicized security vulnerability in the Apache Struts software to go unpatched for months.

After the breach was discovered, Equifax took nearly 6 weeks to notify consumers. Congress, the Federal Trade Commission, and the Consumer Financial Protection Bureau were not notified.

The website set up for consumers was a mess. Equifax tweeted links to a fake website. And the company is only providing 1 year of free credit monitoring services. We are awaiting clarification from Equifax on the credit lock service that it promised to offer at our last hearing.

Those failures should not be a surprise. What incentive does Equifax have to protect consumer data on the front end when consumers aren't its real customers? I have not heard a parade of companies saying that they will refuse to provide Equifax with consumer data or refuse to use its services. This market is failing American consumers, and that is why Congress and consumer watchdogs must step in.

I welcome the CFPB Director, Richard Cordray's call for embedded regulators at the credit reporting agencies. I look forward to the results of investigations into the breach, such as the investigation at the Federal Trade Commission. State attorneys general are also pursuing legal action against the company. And, ultimately, we need stronger legislation.

Last month, I joined several other members of this subcommittee in introducing the Secure and Protect Americans' Data Act. Our bill establishes data security requirements to protect consumers' personal information. That includes special requirements for data brokers like Equifax that collect consumer data often without the consumers' knowledge. And it empowers the Federal Trade Commission to enforce those regulations with civil penalties.

Our bill requires timely notification to State and Federal law enforcement agencies and to consumers when a data breach occurs.

Finally, our bill requires meaningful remedies for breach victims. Victims would be entitled to 10 years of free credit monitoring or quarterly credit reports. And our bill enables breach victims to control access to their personal information and credit reports at no charge.

Our legislation would be a good first step, but I am interested in further action the Congress could take. In written testimony, Mr. Schneier calls for making credit freezes the default so that consumers are opting in to have their data shared rather than paying to opt out.

I expect the industry to engage with these ideas, given the problems consumers face. Old excuses that this is too big a change from the status quo don't cut it anymore.

On October 12, the Democratic members of the subcommittee requested a hearing with current Equifax employees. We also called for advancing bipartisan data security legislation through the committee by the end of this year. And, Chairman Latta, I repeat that call today. Our subcommittee has been bipartisan in demanding answers for breach victims. We should now be bipartisan in pursuing action. I stand ready to work with you on real solutions to protect American consumers.

And thank you for the latitude you have given me, and I yield back.

Mr. LATTA. Well, thank you very much.

The gentlelady does yield back.

And the Chair now recognizes the chairman of the full committee, the gentleman from Oregon, for 5 minutes.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. I thank the chairman. And thank you for your leadership on this and many other issues that we have successfully moved through.

This morning, we are here to discuss the topic of protecting America's data in the digital age.

The advent of new technologies has reduced barriers and eased the ability of consumers to access credit and make needed purchases in ways unimaginable not very long ago. In literally minutes, using one's phone, Americans can procure a loan to purchase a refrigerator, a car, or even a home. The most remarkable thing about this is how unremarkable it has become.

As with any invention, the technological innovations that have facilitated access to credit bring with them new perils. As this committee explored in our hearing last month, Equifax, the credit reporting agency entrusted to safeguard the most important financial data of millions of Americans, instead allowed hackers to access that information through their failure to implement a software patch that had been brought to their attention by the Department of Homeland Security. There is no excuse for that.

And, in fact, consumers all over America now are trying to figure out what do they do next. We had a conversation of that in my own household this weekend. A relative of mine and we have been breached. Everybody is going, "Now what do I do? And why do I have to pay? And what do I have to sign up—where do I go?" This has to get fixed. Enough.

Consumers are the one that are getting taken to the woodshed here. Companies are making billions of dollars off of our data, and we have had it. And we want to do the right thing; we don't want to do what Government often does, which is completely overreact and create a whole new regulatory regime that doesn't work. But let the message go out: This is serious stuff, and consumers are dramatically affected. They are inconvenienced, and it becomes costly to them.

Unfortunately, the Equifax incident was only one example of the keepers of sensitive data failing to do their duty. For millions of current and former U.S. Government employees, including many people in this room, the Federal Office of Personnel Management

similarly failed to live up to its trust to protect their most sensitive data. The OPM breach allowed hackers to access data used by the U.S. Government to determine whether a security clearance could be granted, including the consumer credit information, demonstrating that even the Government struggles to protect its most sensitive data.

These incidents and others like them demonstrate the challenges of protecting consumer information in this digital age. We know it is not easy. They also remind us of how high the stakes are and how critically important it is that Americans know that when they fill out an application to obtain credit they are not exposing their most personal information to bad actors all over the world.

There are a host of laws on the books already that require compliance—let's not lose sight of that—and that furnishers of consumer credit informations are required to take steps to secure the data already under the law. The Gramm-Leach-Bliley Act prohibits financial institutions from disclosing non-public information without the consumers' consent. That is a law. The Fair Credit Reporting Act deems the unauthorized disclosure of consumer reports to be, quote, "an unfair or deceptive act or practice." That is a law.

The Dodd-Frank Act created an entirely new Federal bureaucracy, the Consumer Financial Protection Bureau, and charged it, among other duties, with the task of protecting consumer financial information. Despite these new and sweeping powers, the Bureau seemed completely unaware that a company had failed to implement the necessary software patch that could have saved Americans' data from hackers.

As I noted at the Equifax hearing last month, you can't fix stupid. But, surely, we can do better. Despite all these existing laws and authorities, Equifax allowed the most sensitive consumer credit information of 145 million Americans to be exposed. Equifax's entire business model is predicated on collecting, maintaining, and securing individuals' private financial transaction history. It failed, and now Equifax must face serious consequences.

All of us, I am sure, are interested in any insights our witnesses can provide into how, despite these policies and procedures, incidents like the Equifax breach still happen. There are longstanding Federal, State, and private data security standards and requirements for protecting Americans' sensitive financial data. I am interested in learning more about any gaps or areas for improvement. The instantaneous ability to obtain credit is a remarkable blessing in the electronic age, but it doesn't work when your data are stolen and sold on the dark net. Our ability to obtain credit is only as strong as our data protection.

So I appreciate our witnesses today. And I especially appreciate our substitute witness, who at the last minute made accommodations to share your knowledge with us. Thank you. I am sorry the witness that we had scheduled had to leave, violently ill. And so we appreciate, on short notice, your ability to come and help inform us in our work.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

This morning we are here to discuss the topic of protecting Americans' data in the digital age. The advent of new technologies has reduced barriers and eased the ability of consumers to access credit and make needed purchases in ways unimaginable even a few generations ago.

In literally minutes, using only one's phone, Americans can procure a loan to purchase a refrigerator, a car, or even a house. The most remarkable thing about this is how unremarkable it has become.

As with any invention, the technological innovations that have facilitated access to credit bring with them new perils. As this committee explored in our hearing last month, Equifax, a credit reporting agency entrusted to safeguard the most important financial data of millions of Americans, instead allowed hackers to access that information through their failure to implement a software patch that had been brought to their attention by the Department of Homeland Security.

Unfortunately, the Equifax incident was only one example of the keepers of sensitive data failing to do their duty. For millions of current and former U.S. Government employees, including many people in this room, the Federal Office of Personnel Management similarly failed to live up to its trust to protect their most sensitive data.

The OPM breach allowed hackers to access data used by the U.S. Government to determine whether a security clearance should be granted, including consumer credit information, demonstrating that even the Government struggles to protect its most sensitive information.

These incidents and others like them demonstrate the challenges of protecting consumer information in the digital age. They also remind us of how high are the stakes, and how critically important it is that Americans know that when they fill out an application to obtain credit they are not exposing their most personal information to the world.

There are a host of laws on the books that require the compilers and furnishers of consumer credit information to take steps to secure that data. The Gramm-Leach-Bliley Act prohibits financial institutions from disclosing non-public information without the consumer's consent.

The Fair Credit Reporting Act deems the unauthorized disclosure of consumer reports to be an "unfair or deceptive act or practice."

The Dodd Frank Act created an entirely new Federal bureaucracy, the Consumer Financial Protection Bureau, and charged it, among other duties, with the task of protecting consumer financial information.

Despite these new and sweeping powers, the Bureau seemed completely unaware that the company had failed to implement the necessary software patch that could have saved Americans' data from hackers.

As I noted at the Equifax hearing last month, "you can't fix stupid." But surely we can do better.

Despite all of these existing laws and authorities, Equifax allowed the most sensitive consumer credit information of 145 million Americans to be exposed.

There is no excuse.

Equifax's entire business model is predicated on collecting and maintaining individual's private financial transaction history. It failed, and now Equifax must face serious consequences.

All of us, I am sure, are interested in any insights our witnesses can provide into how, despite these policies and procedures, incidents like the Equifax breach still happen. There are long-standing Federal, State and private data security standards and requirements for protecting Americans' sensitive financial data. I am interested in learning about any gaps or areas for improvement.

The instantaneous ability to obtain credit is a remarkable blessing that remains all too unavailable for most people living in less technologically advanced places. But for the companies and networks that make this privilege possible comes great responsibility.

Our ability to obtain credit is only as strong as our data protection. In the cyber world foxes are always trying to break into the henhouse. It is our duty, and the duty of the possessors of sensitive consumer information, to make sure we have a strong fence.

I look forward to hearing from our witnesses.

Mr. WALDEN. And, with that, Mr. Chair, I yield back the balance of my time.

Mr. LATTA. Well, thank you very much.

The gentleman yields back the balance of his time.

The Chair now recognizes the ranking member of the full committee, the gentleman from New Jersey, for 5 minutes.

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

Mr. PALLONE. Thank you, Mr. Chairman.

I am glad we are holding this hearing, and I hope the committee will focus on how the practices of the credit reporting and data collection industries affect consumers.

But today's hearing should not take the place of additional hearings on the data breach at Equifax. Too many questions remain unanswered, and that is why every Democratic member of this subcommittee wrote to you, Mr. Chairman, requesting additional hearings with current Equifax executives.

The Equifax breach exposed more than 145 million Americans to lifelong threats resulting from their personal information being exposed. Equifax says that it is, and I quote, "taking responsibility for its failures," but Equifax is only providing victims with protections for 1 year. It refuses to give people meaningful control over how Equifax shares and sells the personal information that it collects. And that is not taking responsibility; it is taking advantage, in my opinion.

Consumer reporting agencies collect vast amounts of personal information on almost every American, including children. And this is the information that determines whether someone gets a job or a new home or can afford medical care. And these companies are data brokers, too, selling all of that information to advertisers and others.

You and I are not their customers. We are the product. These companies make their money selling our information to other companies, often without our knowledge and certainly without our approval. So they have no reason to limit the information they collect, to limit sharing or selling of that information, or to properly secure it.

Cyber attacks happen on an hourly basis, with more than 1,100 this year alone. Consumer reporting agencies and data brokers make rich targets for hackers because of the sensitivity and quantity of information they hold. And those companies know it. In fact, it was reported that Equifax was warned by a security researcher in late 2016 that Equifax was vulnerable to attack, but Equifax did nothing and had no incentive to do anything.

Right now, there are gaping holes in the laws and regulations when it comes to collecting and securing our personal information. The bill that Ranking Member Schakowsky and I introduced, the Secure and Protect Americans' Data Act, would close some of these loopholes.

It would provide the Federal Trade Commission with the authority to assign monetary penalty against companies that fail to protect personal information or who fail to provide timely and meaningful notice to consumers that their information has been stolen. It would also give additional protections to victims after a breach. The bill would require that companies that failed to secure individ-

uals' personal information provide free credit freezing or locking to a victim for at least 10 years after a breach.

So we all need to reexamine this industry's approach to consumer protection, including on issues like forced arbitration and the Federal Government's examination or auditing of these companies. We should also look at freezing credit reports by default, ensuring the data that is collected is actually correct, and give people control over their own personal information.

Now, in our hearing and again today, on the Equifax breach, Chairman Walden said that, and I quote, "we can't fix stupid." But we have seen over and over again that breaches are not the result of stupidity. They happen because these companies choose not to invest in security. And, ultimately, it is the American people that pay the price for that choice.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

I'm glad we are holding this hearing, and I hope the committee will focus on how the practices of the credit reporting and data collection industries affect consumers. But today's hearing should not take the place of additional hearings on the data breach at Equifax. Too many questions remain unanswered. And that's why every Democratic member of this subcommittee wrote to you, Mr. Chairman, requesting additional hearings with current Equifax executives.

The Equifax breach exposed more than 145 million Americans to lifelong threats resulting from their personal information being exposed. Equifax says that it is "taking responsibility" for its failures. But Equifax is only providing victims with protections for 1 year. It refuses to give people meaningful control over how Equifax shares and sells the personal information that it collects. That's not "taking responsibility." It's taking advantage.

Consumer reporting agencies collect vast amounts of personal information on almost every American, including children. This is the information that determines whether someone gets a job or a new home, or can afford medical care. And these companies are data brokers too, selling all of that information to advertisers and others.

You and I are not their customers. We are the product. These companies make their money selling our information to other companies, often without our knowledge and certainly without our approval. So they have no reason to limit the information they collect, to limit sharing or selling of that information, or to properly secure it.

Cyberattacks happen on an hourly basis, with more than eleven-hundred this year alone. Consumer reporting agencies and data brokers make rich targets for hackers because of the sensitivity and quantity of information they hold. And those companies know it. In fact, it was reported that Equifax was warned by a security researcher in late 2016 that Equifax was vulnerable to attack. Equifax did nothing and had no incentive to do anything.

Right now, there are gaping holes in the laws and regulations when it comes to collecting and securing our personal information. The bill that Ranking Member Schakowsky and I introduced, the Secure and Protect Americans' Data Act, would close some of those holes. It would provide the Federal Trade Commission with the authority to assign monetary penalties against companies that fail to protect personal information or who fail to provide timely and meaningful notice to consumers that their information has been stolen. It would also give additional protections to victims after a breach. The bill would require that companies that failed to secure individuals' personal information provide free credit freezing or locking to a victim for at least 10 years after a breach.

We also need to reexamine this industry's approach to consumer protection, including on issues like forced arbitration, and the Federal Government's examination or auditing of these companies. We should also look at freezing credit reports by default, ensuring the data that is collected is actually correct, and give people control over their own personal information.

In our hearing on the Equifax breach, Chairman Walden said that we "can't fix stupid," but we have seen over and over again that breaches are not the result of

stupidity. They happen because these companies choose not to invest in security. Ultimately, it's the American people that pay the price for that choice.

Thank you, I yield back.

Mr. PALLONE. I yield the remainder of my time to Congresswoman Matsui.

Ms. MATSUI. Thank you, Ranking Member Pallone. And I am very pleased to cosponsor the Secure and Protect Americans' Data Act that you introduced with Ranking Member Schakowsky.

The need for data security and breach notification requirements are not new. California passed notification legislation a decade and a half ago. But 15 years later, many Americans don't know what happens to their online data, as the Equifax breach has shown us.

In an event that sensitive personal data maintained on an information system is breached, there is no comprehensive Federal law that will protect consumers. That is absolutely unacceptable.

Consumers deserve to know more about how their information is held once it is entered online. It may be that a comprehensive profile of my constituents' online activity could be compiled without them having any knowledge of how or for what purpose that data is being used. Consumers deserve a Federal backstop when that data is compromised.

I look forward to working with the committee on ideas to best provide that certainty to Americans.

Thank you, and I yield back.

Mr. PALLONE. Thank you.

And I yield back, Mr. Chairman.

Mr. LATTA. Thank you very much.

The gentleman yields back the balance of his time, and this now concludes our Member opening statements. The Chair reminds Members that, pursuant to committee rules, all Members' opening statements will be made part of the record.

Additionally, I ask unanimous consent that the Energy and Commerce Committee members not on the Subcommittee on Digital Commerce and Consumer Protection be permitted to participate in today's hearing.

Without objection, so ordered.

Again, I want to thank our witnesses for being with us today and taking time to testify on this very important matter before the subcommittee. Today's witnesses will have the opportunity to give 5-minute opening statements, followed by a round of questions from our members.

Our witness panel for today's hearing will include: Mr. Francis Creighton, who is the president and CEO of the Consumer Data Industry Association; Mr. James Norton, adjunct lecturer at the Johns Hopkins University; Mr. Bruce Schneier, who is the adjunct lecturer in public policy at the Harvard Kennedy School; and Ms. Anne Fortney, who is partner emeritus at Hudson Cook.

And, again, I would like to again thank Mr. Norton for his last-minute replacement of Mr. Greene, who informed the subcommittee that he was unable to testify because of illness. So we appreciate it.

And before we get started, again, our witnesses will have 5 minutes.

If you would like to pull the microphone up close and press the button.

And, Mr. Creighton, you are recognized for 5 minutes. Thanks again for your testimony today.

STATEMENTS OF FRANCIS CREIGHTON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION; JAMES NORTON, ADJUNCT LECTURER, JOHNS HOPKINS UNIVERSITY ZANVYLL KRIEGER SCHOOL OF ARTS AND SCIENCES; BRUCE SCHNEIER, FELLOW AND LECTURER, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD KENNEDY SCHOOL, AND FELLOW, BERKMAN CENTER FOR INTERNET AND SOCIETY AT HARVARD LAW SCHOOL; AND ANNE P. FORTNEY, PARTNER EMERITUS, HUDSON COOK, LLP

STATEMENT OF FRANCIS CREIGHTON

Mr. CREIGHTON. Thank you.

When I took this position with CDIA back in May, I was excited to come here because I wanted to work on an issue I am passionate about: How do we bring more people out of the financial shadows and into the regulated financial system? Consumer reporting is one of the best ways to achieve that goal, and I am excited to have the opportunity to tell that story.

But the news that was revealed on September 7 changed that conversation. The scale of the criminal attack at Equifax is breathtaking, and, like you, I want to better understand what happened and make sure it never happens again.

But in the wake of the attack, we have heard a number of statements that go beyond making sure this doesn't happen again, that somehow the credit reporting system is unregulated and that consumers are getting ripped off. Nothing could be further from the truth.

First, this industry is highly regulated. My written statement goes into more detail, but we are subject to the Fair Credit Reporting Act, one of the most important and strongest consumer protection statutes on the books today. FCRA subjects reporting companies to comprehensive regulatory and consumer protection regimes. The FCRA protects privacy, 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, the nationwide consumer reporting agencies are subject to the FTC's safeguards rule as nonbank financial institutions under the Gramm-Leach-Bliley Act. We are also regulated and face enforcement by the State attorneys general, contractual obligations from our financial institution customers, make sure we meet the requirements of the Federal Financial Institutions Examination Council.

At every level, this is a well-regulated industry. If in the course of the investigation we find a regulatory gap in a particular area, we pledge to work with you to address it. Protecting consumer data is the most important thing we do. It is not just good for business; it is the right thing to do.

But if this were just a question of regulation, that would be one thing, but since the hack, we have heard people suggest that maybe we don't need a consumer reporting system at all. Our credit reporting system today is the envy of the world. It is one of the main reasons American consumers have such a diverse range of lenders and products from which to choose.

This stands in stark contrast to many other financial systems, including those in developed nations. American consumers have access to the most democratic and fair credit system ever to exist. 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 how they personally have handled credit. So when a family tries to buy a house for the first time, they can access the right mortgage for their own personal needs. A young person who comes here to work on the Hill and has to buy a car to get to work can go to an auto dealer and drive off the lot the same day even if she or he has never been to this area. A young family can access credit through a mainstream financial institution rather than depending upon shadowy lending services.

Without access to a full credit report, lenders, landlords, community banks, credit unions, insurance companies, and others won't know how a consumer has handled their obligations in the past unless those service providers know the customer personally.

Credit reports are also a check on human bias and assumptions. They provide lenders with facts that contribute to equitable treatment for consumers. CDIA members establish an accountable and colorblind system for judging creditworthiness. Without this system, subjective judgments could be based on factors other than the fact of creditworthiness.

Today's credit reporting system has made it possible for middle-class consumers to get credit at rates that previously were reserved only for the wealthy. Credit reporting companies are innovating to solve the problem of the unbanked, thin-file, and credit-invisible consumers who have not had a chance to participate in the mainstream financial system.

This is a system that works whether you are at a global bank or at a community-based credit union, because companies share critical information across the system to benefit everyone. In one sense, lenders take their sensitive customer information and share it with a trusted third party so that another financial institution, potentially a competitor, can use that information to make a more informed lending decision. This results in lower prices, more choices for consumers, and a safer and sounder financial system.

Our individual credit reports tell the story of our individual choices. They are neither positive nor negative. They are our best attempt at an accurate portrait of what we individually have done. And they offer the tools lenders and others need to make judgments about how a particular person will handle his or her obligations in the future.

Thank you for having me here today. I look forward to your questions today and in the future.

[The prepared statement of Mr. Creighton follows:]

Statement of Francis Creighton

President & CEO

Consumer Data Industry Association

Before the

Subcommittee on Digital Commerce and Consumer Protection

Committee on Energy and Commerce

United States House of Representatives

Hearing on

"Securing Consumers' Credit Data in the Age of Digital Commerce"

November 1, 2017

Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee, thank you for the opportunity to appear before you.

My name is Francis Creighton, and in May I became the 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. We educate policymakers, regulators, consumers and others on how the responsible use of consumer data empowers economic opportunity.

With more than two-thirds of U.S. gross domestic product coming from consumer spending, CDIA member products are used in billions of transactions each year and expand consumers' access to financial services in a manner that is innovative and focused on their needs.

Consumers today have access to the most democratic and fair credit system ever to exist. 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. This means that when a family tries to buy a house for the first time, they are going to be able to access the right mortgage for their own personal needs. A young person who has a new job and has to buy a car to get to work can go to an auto dealer and drive off the lot even if she or he has no physical history in

that community. Lower income families can access credit through mainstream financial institutions rather than depending upon shadowy lending services.

Today's credit reporting system has made it possible for many middle-class consumers to get credit at rates that previously would have been reserved for the wealthy. 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. In fact, credit reporting companies continue to innovate to solve the problem of the "unbanked" or "credit invisible" consumers, who have not had a chance to participate in the mainstream financial system because they have "thin" or no credit files. By expanding the kinds of information that we collect, we are able to give lenders and others information that allows more consumers to access traditional loans and bank products.

Our credit reporting system today is the envy of the world, and other countries actively work to emulate what we do here. It is one of the main reasons American consumers have such a diverse range of lenders and products from which to choose. This stands in stark contrast to many other financial systems, even those in developed nations.

This is a system that works uniquely well for the consumer. Some have suggested that consumers should have the ability to "opt out" of the credit reporting system.

While this may sound attractive at first blush, it would cause massive problems for the credit markets. Consumers effectively opt in whenever they open a credit account; lenders tell consumers in their loan agreements that they will be reporting information to credit bureaus, and then remind them every year with their Gramm-Leach-Bliley Act-mandated annual privacy notice. Lenders have a business incentive to make sure borrowers understand that this information is being shared, as they want to ensure that borrowers understand that there are additional consequences if a borrower does not meet her or his obligation.

Most consumers pay their bills on time; choosing to "opt out" of the system would mean that someone who has always paid their bills on time would have no credit report available reflecting that fact when they seek out new credit. Lenders would have no way to judge whether an individual applying for credit has paid their bills or not. Creditors and other users of credit reports would find it difficult to assess risk in the larger population if there was a sense that 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 the greater risk faced. And the consumer who has been consistently making the right choices would lose out.

Information is held on credit reports for limited periods of time. If someone closes their accounts and does not access credit, then after seven years, their credit file will become "thin," because they have no outstanding credit. And if they applied for

credit at that point they would likely face the same problems that some in Congress have been trying to address through legislation aimed at helping the "unbanked."

In creating and affirming the Fair Credit Reporting Act over the years, Congress weighed the privacy implications of information sharing and access with the economic benefits to consumers of a robust and efficient credit system, and the safety and soundness of the banking sector. The result is a credit system that other nations seek to emulate: a detailed regulatory regime that limits the sharing of information for permissible purposes only and strict requirements on accuracy, consumer access and correction. Our consumer 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.

Ultimately, our individual credit reports tell the story of our individual choices. They are neither positive nor negative; they are simply our best attempt at an accurate portrait of what we have done, and they give lenders and others the tools they need to make judgements about how a particular person will handle her or his obligations in the future. Because credit reports are always absorbing 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.

Without ready access to a consumer report, lenders, landlords, community banks, credit unions, insurance companies, and others have no assurance that a consumer has reliably paid obligations in the past, unless those service providers know the customer personally. As Richard Cordray, 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."[1]

The US credit system contributes to the diversity of business model choices American banking consumers enjoy by providing disproportionate benefits to smaller financial institutions like community banks and credit unions, who have access to accurate and complete information on par with that available to very large banks. Our consumer credit system works whether you are at a global bank or a community-based credit union because companies share critical information across the system to benefit everyone.

---

[1] Cordray, Richard. Prepared Remarks by Richard Cordray on Credit Reporting (July 16, 2012) (accessed October 23, 2017), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-by-richard-cordray-on-credit-reporting/.

Credit reports are also a check on human bias and assumptions. These reports provide lenders with a foundation of 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 consumers and safety and soundness of lending institutions – by ensuring the accuracy and completeness of information in consumer reports, and by providing businesses with the information they need to ensure consumers are treated fairly. Without this system, subjective judgements could be based on factors other than the facts of creditworthiness.

In the wake of the 2008 financial crisis, our country has also redoubled our efforts to ensure more disciplined underwriting and that borrowers have an ability to repay. CDIA members provide businesses with the information and analytical tools necessary to manage risk and protect consumers. Credit reports are a key way that we protect the consumer finance system by ensuring that banks are not granting credit to those who cannot afford it. This is why federal bank regulators require lenders and others, such as Fannie Mae and Freddie Mac, to use credit reports to assess the creditworthiness of prospective borrowers. One need only remember back to the overuse of "NINJA" (No Income, No Job or Assets) loans in the last decade's mortgage market, when unscrupulous lenders ignored credit reports in return for higher rates, to see the importance of using credit reports to protect the financial system.

This is an extraordinary system. In one sense, lenders take their sensitive customer information, and share it with a trusted third party, so that another financial institution –potentially a competitor—can access that information to make a better lending decision. And this is all done voluntarily, but within a significant regulatory structure[2]. The resulting competition lowers prices to the consumer.

Data Security Requirements for Credit Reporting Companies

The topic of this hearing is "Securing Consumers' Credit Data in the Age of Digital Commerce." Over the course of the rest of this statement I will share the numerous federal, state and private legal regimes under which credit reporting agencies work to secure data.

The Gramm-Leach-Bliley Act & FTC Safeguards Rule

Congress specifically designated credit reporting agencies as financial institutions that are subject to the information security requirements of the Gramm-Leach-Bliley Act (GLBA), designed in part by the predecessor of this Committee in 1999, and its implementing regulation, the Standards for Safeguarding Customer

[2] Student loan servicers are required to report to credit bureaus by law (20 U.S. Code § 1080a). Fannie Mae and Freddie Mac guidelines require credit reporting. Federal banking regulators have strongly encouraged their regulated communities to participate in credit reporting. Non-bank furnishers of data, such as non-bank auto-lenders, landlords and others, participate in the system on a voluntary basis.

Information ("Safeguards Rule") promulgated by the Federal Trade Commission (FTC)[3]. 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 consumer[4].

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 any customer information at issue[5].

Financial institutions, including credit reporting agencies, must also designate an employee to coordinate their comprehensive information security program, as well

[3] 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 – i.e., the Federal Reserve, the Office of the Comptroller of the Currency, and the 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).
[4] 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).
[5] 16 C.F.R. § 314.3(a).

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 risks[6]. 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 safeguards[7].

These common-sense provisions are general parameters designed to allow evolving standards to keep pace with the evolving threat landscape. At their inception lawmakers and regulators anticipated that private institutions and the government overseers closest to the battle lines and with the greatest expertise in these matters 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 Act[8]. Pursuant to the FTC Act, the FTC is empowered to take action against any business that engages in "unfair

[6] 16 C.F.R. § 314.4.
[7] 16 C.F.R. § 314.4(d).
[8] 15 U.S.C. § 45.

or deceptive acts or practices" ("UDAP"), which the agency has interpreted to include inadequate data security practices[9].

The FTC requires that a company 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 vulnerabilities[10]." 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 information[11].

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 risk[12]."

---

[9] 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), https://fas.org/sgp/crs/misc/R43723.pdf.
[10] Federal Trade Commission, "Data Security" (accessed October 23, 2017), https://www.ftc.gov/datasecurity.
[11] See, e.g., Federal Trade Commission, "Protecting Personal Information: A Guide for Business" (accessed October 23, 2017), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[12] See Federal Trade Commission, "Privacy and Data Security Update (2016)" (January 2017) (accessed October 23, 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

Fair Credit Reporting Act: Credentialing and Disposal Requirements

The Fair Credit Reporting Act (FCRA) requires that credit reporting companies only provide credit reports to people with a "permissible purpose" to receive such reports, such as credit or insurance underwriting. More importantly, the law requires that every credit reporting company maintain reasonable procedures designed to ensure that credit reports are provided only to permissible people for legitimate purposes. These 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 ChoicePoint[13], 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.

The nationwide credit bureaus, and credit reporting companies generally, take these "credentialing" responsibilities very seriously. In addition, the nationwide credit bureaus have been examined by the CFPB with respect to the strength and resiliency of their credentialing procedures. As a part of their credentialing

[13] 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 October 23, 2017), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

procedures, credit reporting companies maintain detailed written procedures which take into account the risks presented by prospective users and their proposed uses of information. These procedures routinely include:

- site visits to ensure the premises are consistent with the stated business of the prospective customer;
- review of public information sources and public filings to confirm licensure and good standing;
- review of company websites and other public-facing materials;
- checking financial references, including credit reports of owners for certain types of companies, such as those that are not publicly traded;
- specific and detailed contractual representations and warranties, as well as specific certifications, that credit report information will be used only for specified purposes;
- detailed customer on-boarding and training procedures; and
- ongoing monitoring of customers – including transaction testing – to ensure that customers are in fact using credit reports for legitimate and permissible purposes.

In addition to these credentialing requirements, the FCRA prohibits credit reporting companies – and anyone else handling credit report information – from disposing of that information in a manner that is not secure. More specifically, the FTC issued a rule providing that a person who maintains or otherwise possesses

credit report information, or information derived from credit reports, must properly dispose of such information by taking reasonable measures to protect against the unauthorized access to or use of the information in connection with its disposal[14].

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 practices[15]. 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 disclosure[16]. The majority of states require businesses to dispose of sensitive personal information securely[17].

---

[14] See FCRA § 628.

[15] See, e.g., Xavier Becerra, California Attorney General, "Attorney General Becerra: Target Settles Record $18.5 Million Credit Card Data Breach Case" (May 23, 2017), (accessed October 23, 2017), https://oag.ca.gov/news/press-releases/attorney-general-becerra-target-settles-record-185-million-credit-card-data

[16] See National Conference of State Legislatures, "Data Security Laws – Private Sector" (January 16, 2017), (accessed October 23, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[17] See National Conference of State Legislatures, "Data Disposal Laws" (December 1, 2016), (accessed October 23, 2017), 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 information[18]. 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 substantial additional legal requirements that result 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 providers[19].

---

[18] See National Conference of State Legislatures, "Security Breach Notification Laws" (April 12, 2017), (accessed October 23, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[19] See FFIEC, IT Examination Handbook Infobase, "Information Security: Oversight of Third-Party Service Providers," (accessed October 23, 2017), https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers.aspx.

Pursuant to these FFIEC requirements, financial institutions and their auditors subject the nationwide credit bureaus to dozens of 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 DSS[20].

[20] Payment Card Industry Security Standards Council, "Requirements and Security Assessment Procedures, Version 3.2" (April 2016).

All three of the nationwide credit bureaus have been certified by the card networks as "PCI DSS Validated Service Providers," meaning that they are approved to store, process and transmit cardholder data. Service providers that store, process or transmit cardholder data must be registered with the card networks and demonstrate PCI DSS compliance. PCI DSS compliance validation is required every 12 months for all service providers.

The Fair Credit Reporting Act and CFPB Supervision

The federal FCRA has been around for nearly 50 years, with occasional fine tuning, two significant revisions (1996 & 2003) and now (starting in 2012) CFPB supervision and examination of the credit reporting companies for compliance with the FCRA[21].

When the credit reporting industry first began in the United States, there was little standardization in the methods used and types of information collected as it was a decentralized, city-by-city, business. In particular, there was no standard procedure for consumers to find out what was in a credit report and to 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 FCRA, which Congress passed in 1970. The FCRA imposed duties on credit reporting companies (referred to as "consumer

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

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 statute 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 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 victims[22], 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 that provides many protections to consumers. A number of these provisions are designed to protect consumer privacy, such as the aforementioned permissible purpose and credentialing requirements. The 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

[22] FCRA § 609(e).

authorized to receive them, for example, by selling consumers' private information to a litigation opponent or an ex-spouse hoping to find embarrassing information[23].

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 file[24]. The 2003 amendments to the FCRA additionally required nationwide credit bureaus and nationwide specialty 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 corrected[25]. 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. In addition, consumers have the right to dispute the contents of the file, and the credit reporting company is obligated to conduct a reasonable investigation of the dispute[26]. Credit reporting companies must also independently employ reasonable procedures to assure maximum possible accuracy of the information in consumer files[27].

---

[23] FCRA § 607(a).
[24] FCRA § 609.
[25] FCRA § 615(a).
[26] FCRA § 611
[27] FCRA § 607(b).

Finally, in 2012, the CFPB became the first supervisor of the national credit reporting system. 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 reports[28]. Since the CFPB formalized its supervisory authority in January 2012, 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 management" that "will reap benefits for consumers – and the lenders that use consumer reports – for many years to come."[29]

---

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

[29] See CFPB, "Supervisory Highlights: Consumer Reporting Special Edition, Issue 14, Winter 2017 (March 2017) (accessed October 23, 2017), http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

As I have demonstrated through my testimony: this industry is regulated by multiple federal and state laws, enforced by multiple regulators, including the CFPB, FTC, State Attorneys General, banking regulators and more. And still there was a security breach. I am not here to speak for Equifax[30] specifically on the details of that breach but they have been clear in public testimony that they have closed the vulnerability exploited by the criminal hackers.

What I am here to do today is demonstrate the willingness of our industry to work with Congress and the regulatory bodies to ensure the security of consumer information. We will do everything in our power to ensure our customers have confidence their data is in good hands.

In conclusion, data security is not just our regulatory and legal obligation; it is good business. And it is just the right thing to do – for consumers, for our customers and for the entire financial system.

I look forward to your questions, today and into the future.

[30] Officials at Equifax have had the opportunity to review this testimony, though they did not comment on its preparation.

Mr. LATTA. Again, thank you very much for testifying before us today.

And, Mr. Norton, you are recognized for 5 minutes.

STATEMENT OF JAMES NORTON

Mr. NORTON. Thank you, Chairman Latta, Ranking Member Schakowsky, and members of the subcommittee. Thank you very much for inviting me to testify before you today.

My name is James Norton, and I am the founder and president of Play-Action Strategies, a homeland security consulting firm here in Washington, DC. I am also a member of the Johns Hopkins University faculty, teaching graduate courses on homeland security and cybersecurity.

Previously, I served in multiple positions at the Department of Homeland Security under President George W. Bush, including as Deputy Assistant Secretary of Legislative Affairs. I was a member of the Department's first team tasked with confronting the then-nascent cybersecurity threat.

My testimony will focus on how attacks like the one that led to the Equifax breach fit into the larger cybersecurity context and what can be done to strengthen cybersecurity protections on the front end.

Today, cybersecurity threats are pervasive, and any company or institution that houses large amounts of personal data is a potential target. Each year, hackers and other bad actors launch millions of attacks on cyber infrastructure maintained by governments, businesses, and individuals.

Current cyber threats take many forms and target a range of vulnerabilities, increasing the complexity of cybersecurity missions. Attacks like the Equifax breach, the WannaCry ransomware attack, and the Yahoo breach in 2013–2014 are more widespread and complex than earlier intrusions, demonstrating that bad actors are becoming more sophisticated in their efforts. So far, cybersecurity protections have largely failed to keep pace.

While security frameworks like those laid out in the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act are important guideposts and should be maintained, lawmakers should resist the temptation to put in place rules and regulations that requires companies and institutions to take specific federally prescribed actions to address cybersecurity issues resulting in limited flexibility for private-sector companies to respond to emerging threats. Instead, I would encourage officials to commit themselves to working collaboratively with businesses and consumers to share best practices and raise awareness about the scope and sophistication of cyber threats.

To help meaningfully address cybersecurity challenges, I offer the following recommendations for the subcommittee:

The Federal Government should take the lead in convening relevant stakeholder meetings to develop and share best practices, including an examination of how efforts currently underway within the Federal Government and in the private sector can be adapted for applications in other sectors, as well as help businesses better understand the national security threat with the intelligence that is available to the Government.

Government officials and private-sector leaders must make a more concerted effort to ensure that consumers and even other businesses, especially small-business owners, are aware of the threat and the tools that are publicly available in the marketplace to reduce the vulnerability.

Businesses must encourage a path to integrate cybersecurity into their companies' culture through regular training and updates, which obviously was lacking with Equifax.

I thank the committee for holding this important hearing, and I look forward to your questions. Thank you.

[The prepared statement of Mr. Norton follows:]

Securing Consumers' Credit Data in the Age of Digital Commerce

U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

Testimony of James Norton
Founder and President, Play-Action Strategies LLC

November 1, 2017

Introduction

Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee, thank you very much for inviting me to testify before you today.

My name is James Norton, and I am the founder and president of Play-Action Strategies LLC, a homeland security and cybersecurity consulting firm here in Washington, D.C. Previously, I served in several positions at the Department of Homeland Security ("DHS") under President George W. Bush, including as Deputy Assistant Secretary of Legislative Affairs. During the stand up of DHS, I was deeply engaged in the creation of the Department's first team dedicated to confronting the then-nascent cybersecurity threat. After my service at DHS, I continued to work extensively on cybersecurity issues, both in my consultancy and as an adjunct faculty member at Johns Hopkins University's Zanvyl Krieger School of Arts and Sciences Advanced Academic Programs, where I teach courses on homeland security, cybersecurity policy, and congressional affairs. To be clear however, today I am expressing my personal views. I am appearing in my individual capacity and not as a representative of any company or organization.

In early October, this Subcommittee held a hearing to examine the recent Equifax data breach that exposed the potentially sensitive information of more than 140 million Americans. I applaud the Subcommittee for convening this subsequent

hearing to discuss how – given what we know now – we can work together to better protect personal information that is in the hands of credit reporting agencies (CRAs) and other consumer institutions. My testimony will focus on how attacks like the one that led to the Equifax breach fit into the larger cybersecurity context and what can be done to strengthen cybersecurity protections on the front end.

Current Landscape

Today, cybersecurity threats are pervasive, and any company or institution that houses large amounts of personal data is a potential target. Each year, hackers and other bad actors launch millions of attacks on cyber infrastructure maintained by governments, businesses, and individuals. One analysis estimates that the impact of cybercrime will cost $6 trillion annually by 2021, including "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."[1]

Current cyber threats take many forms and target a range of vulnerabilities, increasing the complexity of the cybersecurity mission. Attackers may leverage existing software vulnerabilities to gain access to data – as happened in the Equifax attack, they may use "spear phishing" or other means to introduce malware that will infect a computer or network, ransomware can lock individual user data until a "ransom" is paid and the information unlocked by the attackers, and increasingly, bad actors are perpetrating denial of service attacks intended to massively disrupt

[1] 2017 Cybercrime Report, Cybersecurity Ventures, October 19, 2017

web service. Along with multiple types of attacks, the profusion of networked devices offers bad actors multiple entry points to perpetrate attacks. The complexity of the cyber threat landscape, and the speed with which new threats evolve, represents one of the greatest challenges facing officials, businesses, and consumers is the rapidly changing cyber threat landscape. Attacks like the Equifax breach, the WannaCry ransomware attack, and the Yahoo breach in 2013-14 are more widespread and complex than earlier intrusions, demonstrating that bad actors are becoming more sophisticated in their efforts. So far, cybersecurity protections have largely failed to keep pace.

The private sector's cybersecurity problems cannot be blamed solely, or even mostly, on a lack of federal regulation. Instead, a root cause of the problems is a failure of organizations, private sector and governmental, to establish a culture of cybersecurity awareness. Organizations should not assume that employees understand cybersecurity and, as such, must be diligent about training employees on their role in keeping information protected — with an emphasis on recognizing phishing and spear phishing emails that are designed to trick them into giving away credentials or installing malware. Training should also cover smart social media practices, ground rules for downloading software, and the importance of strong passwords. Beyond formal training sessions, talking about security regularly at staff meetings, encouraging workers to think about security at the front end of projects, and displaying policies and tips around the office can help build a cybersecurity culture.

Federal Role

While the federal government has an important role to play in supporting private sector cybersecurity efforts and protecting consumer information, it is important to acknowledge that the government is still working to secure its own systems – for example, I recently testified in front of the House Science, Space, and Technology Committee regarding the issues surrounding the federal government's use of Kaspersky software. While security frameworks like those laid out in the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA) are important guideposts and should be maintained, federal lawmakers should resist the temptation to put in place rules or regulations that require companies and institutions to take specific, federally-prescribed actions to address cybersecurity issues, resulting in limited flexibility for private sector companies to respond to emerging threats. In other contexts, we have seen critical infrastructure sectors struggle to balance the implementation of federal requirements with emerging threats, with a notable example being airport security. Creating restrictive cybersecurity requirements would likely have an adverse impact on the marketplace, and any specific steps developed now would likely become quickly obsolete.

Instead, federal lawmakers and officials should commit themselves to working collaboratively with businesses and consumers to share best practices and raise awareness about the scope and sophistication of cyber threats. Many of the cybersecurity challenges faced by companies and consumers are a direct result of a lack of knowledge and resources; as the Equifax breach demonstrates, our cybersecurity posture largely remains reactive, rather than proactive. Those of us

who follow cybersecurity issues have long wondered when the tipping point will be reached. That is, when does the cyber threat become real and tangible enough for us to stop being reactionary and finally dedicate sufficient resources and talent to get ahead of it? I believe that moment is now.

Recommendations

- The federal government should take the lead in convening relevant stakeholders to develop and share best practices, including an examination of how efforts currently underway within the federal government and in the private sector can be adapted for applications in other sectors. In order to expedite the flow of information, the government should consider innovative solutions, potentially including the expansion of existing exchange programs that allow federal employees work on-site with private cybersecurity companies and specialists from those companies work with agency and department personnel to strengthen their cybersecurity infrastructure.
- Government officials and private sector leaders must make a more concerted effort to ensure that consumers (and even other businesses, especially small business owners) are aware of the threats and the tools that are publicly available in the market place to reduce vulnerability. Comparatively simple steps – like regularly changing passwords and ensuring that security software is up to date – can meaningfully reduce the vulnerability of individual devices to cyber attacks. In addition, consumers can take common sense steps, like regularly monitoring their credit reports, to ensure they are

aware of any irregularities that may indicate an intrusion. Finally, federal, state, and local officials can work together to ensure that individuals impacted by cyber attacks know the process for responding, based on the type of attack and what information may have been compromised – financial, medical, etc.

Mr. LATTA. Thank you very much for your testimony.

And, Mr.—I want to make sure I am pronouncing your name—it is "Schneier"? "Schneier"?

Mr. SCHNEIER. Rhymes with "frequent flyer."

Mr. LATTA. OK.

Ms. SCHAKOWSKY. I said it wrong too. I added a D.

So "Schneier," right?

Mr. LATTA. We apologize. We want to make sure we get it right.

You are recognized for 5 minutes. Thank you very much for testifying today.

STATEMENT OF BRUCE SCHNEIER

Mr. SCHNEIER. Thank you for having me.

I am Bruce Schneier. I am a fellow and lecturer at the Harvard Kennedy School. I am associated with the Berkman Center at Harvard. I also work for IBM. I am speaking for none of them. And, actually, it is probably best if we just don't tell IBM that I am here.

The Equifax breach was bad. We have heard a lot of the details. This was very sensitive information about half of our country. And Equifax security really was laughably bad, both before, during, and after the attack. This is also not the first time. There is a Forbes article that outlines breach after breach from Equifax.

So the question I ask is, what is going on? We have this large data-broker industry whose job is to collect information about us to sell to other people. We are talking about financial information, but it is actually much more than that: information about our interests, about what we do, about what we do on the internet, things we buy, places we go. It is thousands and thousands of data points about all of us, some of them very intimate, that are wanted by others and are collected, sorted, collated, and sold without our knowledge and consent.

And the market can't fix this. A couple of people have said that we are not the customers. And that is correct; we are not Equifax's customer.

Chairman Walden said, you know, there is no excuse for stupid. There actually is an excuse for what Equifax did. If you are the CEO of Equifax—and he was here—and your choice is to either save 5 percent on your budget by having lax security and taking the chance or spending the money, you are going to take the chance. You are rewarded by coming in under budget. As long as your customers don't complain—and none of them did—that is not a problem. Because we are the product, we are not protected. And that is why this is not something that a market can fix.

The CEO left with an $18 million pension. He did OK. His decision was arguably the correct one in this environment.

All right. So what should we do here? There is a 2014 FTC report on data brokers. It is worth picking up and reading again. It talks about more transparency and more customer control over their data.

I would like it if you would fund research into the actual harms that come from these breaches. One of the problems in lawsuits from customers is that proving harms is hard. If you were the victim of identity theft in 6 months, was it because of Equifax or be-

cause of half a dozen other breaches? You don't know. And without that direct connect, courts will throw out cases.

I would like to see a nationwide credit freeze, where credit information is given upon permission. There is no reason why my credit should be given out without my permission. If I am applying for a car or I am applying for a mortgage, I am going to know, so I should be able to do that.

I would like some kind of data minimization. We talked about opt out. Be careful, though. Opt out often doesn't mean opt out. In many of these cases, when you opt out, you opt out your data being given away—not being collected, not being stored. You will be just as vulnerable when there is a breach if you opted out as if you opted in. So be careful what "opt out" means.

I would like the FTC to set minimum security standards, financial and nonfinancial.

And avoid questioning if this is too hard. Right now, a lot of these companies operate in Europe. The regulations are much more stringent. Starting next year, we are going to see the GDPR, the generalized data protection regulations, even more stringent. And they can do things there they can bring here.

So a couple of final points.

This has some real foreign trade implications. Right now, there are safe harbor rules that allow us, U.S. companies, to collect data on Europeans. If we show that we are incompetent at it, those rules are going to be dropped, and we are going to have a lot of problems for our U.S. companies doing business overseas.

And this has national security implications as well. Someone mentioned that China went after the Office of Personnel Management. They are after data on U.S. citizens. North Korea funds a lot of their stuff using cyber crime. Russia wants our data. The data of all of us, of all of you, are in these databases, and foreign governments want it. To the extent we don't protect it, we are making it easier for them.

If you had half a dozen people standing behind you constantly, taking notes on everything you did, you would notice that, and there would be a law immediately making that illegal. That is what happens today. There are something like 2,500 to 4,000 data brokers, and they are in your computer secretly taking notes, collecting data on everything you do, everything all of us do.

That is a massive industry, and it is invisible. We need to make it visible, and we need to institute some controls. This is not something the market can fix, because we are its product.

Thank you.

[The prepared statement of Mr. Schneier follows:]

Testimony and Statement for the Record of

Bruce Schneier
Fellow and Lecturer, Belfer Center for Science and International Affairs, Harvard Kennedy School
Fellow, Berkman Center for Internet and Society at Harvard Law School

Hearing on "Securing Consumers' Credit Data in the Age of Digital Commerce"

Before the

Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

1 November 2017
2125 Rayburn House Office Building
Washington, DC 20515

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the security of credit data. My name is Bruce Schneier, and I am a security technologist. For over 30 years I have studied the technologies of security and privacy. I have authored 13 books on these subjects, including *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your* World (Norton, 2015). My popular newsletter Crypto-Gram and my blog *Schneier on* Security are read by over 250,000 people.

Additionally, I am a Fellow and Lecturer at the Harvard Kennedy School of Government—where I teach Internet security policy—and a Fellow at the Berkman-Klein Center for Internet and Society at Harvard Law School. I am a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of Electronic Privacy Information Center and VerifiedVoting.org. I am also a special advisor to IBM Security and the Chief Technology Officer of IBM Resilient.

I am here representing none of those organizations, and speak only for myself based on my own expertise and experience.

I have eleven main points:

1. The Equifax breach was a serious security breach that puts millions of Americans at risk.

Equifax reported[1] that 145.5 million US customers, about 44% of the population, were impacted by the breach. (That's the original 143 million plus the additional 2.5 million disclosed a month later.[2]) The attackers got access to full names, Social Security numbers, birth dates, addresses, and driver's license numbers.

This is exactly the sort of information criminals can use to impersonate victims to banks, credit card companies, insurance companies, cell phone companies and other businesses vulnerable to fraud. As a result, all 143 million US victims are at greater risk of identity theft, and will remain at risk for years to come. And those who suffer identify theft will have problems for months, if not years, as they work to clean up their name and credit rating.

2. Equifax was solely at fault.

This was not a sophisticated attack. The security breach was a result of a vulnerability in the software for their websites: a program called Apache Struts. The particular vulnerability was fixed by Apache in a security patch that was made available on March 6, 2017.[3] This was not a minor vulnerability; the computer press at the time called it "critical."[4] Within days, it was being used by attackers to break into web servers. Equifax was notified by Apache, US CERT, and the Department of Homeland Security about the vulnerability, and was provided instructions to make the fix.[5]

---

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[2] https://www.nytimes.com/2017/10/02/business/equifax-breach.html

[3] https://cwiki.apache.org/confluence/display/WW/S2-045

[4] https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/

[5] https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/

Two months later, Equifax had still failed to patch its systems. It eventually got around to it on July 29.[6] The attackers used the vulnerability to access the company's databases and steal consumer information on May 13, over two months after Equifax should have patched the vulnerability.[7]

The company's incident response after the breach was similarly damaging. It waited nearly six weeks before informing victims that their personal information had been stolen and they were at increased risk of identity theft. Equifax opened a website to help aid customers, but the poor security around that—the site was at a domain separate from the Equifax domain—invited fraudulent imitators and even more damage to victims. At one point, the official Equifax communications even directed people to that fraudulent site.[8]

This is not the first time Equifax failed to take computer security seriously. It confessed to another data leak in January 2017. In May 2016, one of its websites was hacked, resulting in 430,000 people having their personal information stolen. Also in 2016, a security researcher found and reported a basic security vulnerability in its main website. And in 2014, the company reported yet another security breach of consumer information. There are more.[9]

3. There are thousands of data brokers with similarly intimate information, similarly at risk.

Equifax is more than a credit reporting agency. It's a data broker.[10] It collects information about all of us, analyzes it all, and then sells those insights. It might be one of the biggest, but there are 2,500 to 4,000 other data brokers that are collecting, storing, and selling information about us—almost all of them companies you've never heard of and have no business relationship with.

The breadth and depth of information that data brokers have is astonishing. Data brokers collect and store billions of data elements covering nearly every US consumer. Just one of the data

---

[6] https://arstechnica.com/tech-policy/2017/09/equifax-cio-cso-retire-in-wake-of-huge-security-breach/

[7] https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/

[8] https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html

[9] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/

[10] https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

brokers studied holds information on more than 1.4 billion consumer transactions and 700 billion data elements, and another adds more than 3 billion new data points to its database each month.[11]

These brokers collect demographic information: names, addresses, telephone numbers, e-mail addresses, gender, age, marital status, presence and ages of children in household, education level, profession, income level, political affiliation, cars driven, and information about homes and other property. They collect lists of things we've purchased, when we've purchased them, and how we paid for them. They keep track of deaths, divorces, and diseases in our families. They collect everything about what we do on the Internet.

4. These data brokers deliberately hide their actions, and make it difficult for consumers to learn about or control their data.

If there were a dozen people who stood behind us and took notes of everything we purchased, read, searched for, or said, we would be alarmed at the privacy invasion. But because these companies operate in secret, inside our browsers and financial transactions, we don't see them and we don't know they're there.

Regarding Equifax, few consumers have any idea what the company knows about them, who they sell personal data to or why. If anyone knows about them at all, it's about their business as a credit bureau, not their business as a data broker.[12] Their website lists 57 different offerings for business: products for industries like automotive, education, health care, insurance, and restaurants.[13]

In general, options to "opt-out" don't work with data brokers. It's a confusing process, and doesn't result in your data being deleted. Data brokers will still collect data about consumers who opt out. It will still be in those companies' databases, and will still be vulnerable. It just don't be included individually when they sell data to their customers.

5. The existing regulatory structure is inadequate.

---

[11] https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

[12] https://www.forbes.com/sites/forrester/2017/09/08/equifax-does-more-than-credit-scores/#1e73610019d8

[13] http://www.equifax.com/business/

Right now, there is no way for consumers to protect themselves. Their data has been harvested and analyzed by these companies without their knowledge or consent. They cannot improve the security of their personal data, and have no control over how vulnerable it is. They only learn about data breaches when the companies announce them—which can be months after the breaches occur—and at that point the onus is on them to obtain credit monitoring services or credit freezes. And even those only protect consumers from some of the harms, and only those suffered after Equifax admitted to the breach.

Right now, the press is reporting "dozens" of lawsuits against Equifax from shareholders, consumers, and banks.[14] Massachusetts has sued Equifax for violating state consumer protection and privacy laws.[15] Other states may follow suit.[16]

If any of these plaintiffs win in the court, it will be a rare victory for victims of privacy breaches against the companies that have our personal information. Current law is too narrowly focused on people who have suffered financial losses directly traceable to a specific breach. Proving this is difficult. If you are the victim of identity theft in the next month, is it because of Equifax or does the blame belong to another of the thousands of companies who have your personal data? As long as one can't prove it one way or the other, data brokers remain blameless and liability free.

Additionally, much of this market in our personal data falls outside the protections of the Fair Credit Reporting Act. And in order for the Federal Trade Commission to levy a fine against Equifax, it needs to have a consent order and then a subsequent violation. Any fines will be limited to credit information, which is a small portion of the enormous amount of information these companies know about us. In reality, this is not an effective enforcement regime.

Although the FTC is investigating Equifax, it is unclear if it has a viable case.[17]

6. The market cannot fix this because we are not the customers of data brokers.

---

[14] https://www.washingtonpost.com/news/business/wp/2017/09/22/after-the-breach-equifax-now-faces-the-lawsuits/?utm_term=.1fd423f6b3aa

[15] http://money.cnn.com/2017/09/12/news/equifax-lawsuit-massachusetts/index.html

[16] http://money.cnn.com/2017/09/19/technology/equifax-legal-issues/index.html

[17] https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/

The customers of these companies are people and organizations who want to buy information: banks looking to lend you money, landlords deciding whether to rent you an apartment, employers deciding whether to hire you, companies trying to figure out whether you'd be a profitable customer—everyone who wants to sell you something, even governments.

Markets work because buyers choose from a choice of sellers, and sellers compete for buyers. None of us are Equifax's customers. None of us are the customers of any of these data brokers. We can't refuse to do business with the companies. We can't remove our data from their databases. With few limited exceptions, we can't even see what data these companies have about us or correct any mistakes.

We are the product that these companies sell to their customers: those who want to use our personal information to understand us, categorize us, make decisions about us, and persuade us.

Worse, the financial markets reward bad security. Given the choice between increasing their cybersecurity budget by 5%, or saving that money and taking the chance, a rational CEO chooses to save the money. Wall Street rewards those whose balance sheets look good, not those who are secure. And if senior management gets unlucky and the a public breach happens, they end up okay. Equifax's CEO didn't get his $5.2 million severance pay, but he did keep his $18.4 million pension. Any company that spends more on security than absolutely necessary is immediately penalized by shareholders when its profits decrease.

Even the negative PR that Equifax is currently suffering will fade. Unless we expect data brokers to put public interest ahead of profits, the security of this industry will never improve without government regulation.

7. We need effective regulation of data brokers.

In 2014, the Federal Trade Commission recommended that Congress require data brokers be more transparent and give consumers more control over their personal information.[18] That report contains good suggestions on how to regulate this industry.

First, Congress should help plaintiffs in data breach cases by authorizing and funding empirical research on the harm individuals receive from these breaches.

---

[18] https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

Specifically, Congress should move forward legislative proposals that establish a nationwide "credit freeze"—which is better described as changing the default for disclosure from opt-out to opt-in—and free lifetime credit monitoring services. By this I do not mean giving customers free credit-freeze options, a proposed by Senators Warren and Schatz[19], but that the default should be a credit freeze.

The credit card industry routinely notifies consumers when there are suspicious charges. It is obvious that credit reporting agencies should have a similar obligation to notify consumers when there is suspicious activity concerning their credit report.

On the technology side, more could be done to limit the amount of personal data companies are allowed to collect. Increasingly, privacy safeguards impose "data minimization" requirements to ensure that only the data that is actually needed is collected. On the other hand, Congress should not create a new national identifier to replace the Social Security Numbers.[20] That would make the system of identification even more brittle. Better is to reduce dependence on systems of identification and to create contextual identification where necessary.

Finally, Congress needs to give the Federal Trade Commission the authority to set minimum security standards for data brokers and to give consumers more control over their personal information. This is essential as long as consumers are these companies' products and not their customers.

8. Resist complaints from the industry that this is "too hard."

The credit bureaus and data brokers, and their lobbyists and trade-association representatives, will claim that many of these measures are too hard. They're not telling you the truth.

Take one example: credit freezes. This is an effective security measure that protects consumers, but the process of getting one and of temporarily unfreezing credit is made deliberately onerous by the credit bureaus. Why isn't there a smartphone app that alerts me when someone wants to access my credit rating, and lets me freeze and unfreeze my credit at the touch of the screen? Too hard? Today, you can have an app on your phone that does something similar if you try to log into a computer network, or if someone tries to use your credit card at a physical location different from where you are.

---

[19] http://money.cnn.com/2017/09/15/pf/warren-schatz-equifax/index.html

Moreover, any credit bureau or data broker operating in Europe is already obligated to follow the more rigorous EU privacy laws. The EU General Data Protection Regulation will come into force, requiring even more security and privacy controls for companies collecting storing the personal data of EU citizens.[21] Those companies have already demonstrated that they can comply with those more stringent regulations.

Credit bureaus, and data brokers in general, are deliberately not implementing these 21st-century security solutions, because they want their services to be as easy and useful as possible for their actual customers: those who are buying your information. Similarly, companies that use this personal information to open accounts are not implementing more stringent security because they want their services to be as easy-to-use and convenient as possible.

9. This has foreign trade implications.

The Canadian Broadcast Corporation reported that 100,000 Canadians had their data stolen in the Equifax breach.[22] The British Broadcasting Corporation originally reported that 400,000 UK consumers were affected;[23] Equifax has since revised that to 15.2 million.[24]

Many American Internet companies have significant numbers of European users and customers, and rely on negotiated safe harbor agreements to legally collect and store personal data of EU citizens.

The European Union is in the middle of a massive regulatory shift in its privacy laws, and those agreements are coming under renewed scrutiny. Breaches such as Equifax give these European regulators a powerful argument that US privacy regulations are inadequate to protect their citizens' data, and that they should require that data to remain in Europe. This could significantly harm American Internet companies.

10. This has national security implications.

---

[20] https://www.cnet.com/news/equifax-trump-white-house-official-replace-social-security-numbers/

[21] http://adage.com/article/datadriven-marketing/eu-privacy-rules-complexity-data-marketers/301854/

[22] http://www.cbc.ca/news/technology/equifax-canada-breach-sin-cybersecurity-what-we-know-1.4297532

[23] http://www.bbc.com/news/technology-41286638

[24] https://www.equifax.co.uk/about-equifax/press-releases/en_gb/-/blogs/equifax-ltd-uk-update-regarding-the-ongoing-investigation-into-us-cyber-security-incident

Although it is still unknown who compromised the Equifax database, it could easily have been a foreign adversary that routinely attacks the servers of US companies and US federal agencies with the goal of exploiting security vulnerabilities and obtaining personal data.

When the Fair Credit Reporting Act was passed in 1970, the concern was that the credit bureaus might misuse our data. That is still a concern, but the world has changed since then. Credit bureaus and data brokers have far more intimate data about all of us. And it is valuable not only to companies wanting to advertise to us, but foreign governments as well. In 2015, the Chinese breached the database of the Office of Personal Management and stole the detailed security clearance information of 21 million Americans. North Korea routinely engages in cybercrime as way to fund its other activities.[25] In a world where foreign governments use cyber capabilities to attack US assets, requiring data brokers to limit collection of personal data, securely store the data they collect, and delete data about consumers when it is no longer needed is a matter of national security.

11. We need to do something about it.

Yes, this breach is a huge black eye and a temporary stock dip for Equifax—this month. Soon, another company will have suffered a massive data breach and few will remember Equifax's problem. Does anyone remember last year when Yahoo admitted that it exposed personal information of a billion users in 2013 and another half billion in 2014?

Unless Congress acts to protect consumer information in the digital age, these breaches will continue.

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

---

[25] https://www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO

Mr. LATTA. We appreciate your testimony this morning.

And, Ms. Fortney, you are recognized for 5 minutes.

STATEMENT OF ANNE P. FORTNEY

Ms. FORTNEY. Thank you.

Good morning. I am Anne Fortney. Thank you for the opportunity to appear before you today.

I am the partner emeritus at Hudson Cook law firm. My career involved more than 40 years' experience with consumer reporting and the credit industry, including service as the Associate Director for Credit Practices at the Federal Trade Commission and as in-house counsel at a retail creditor. I also served as a lawyer consulting clients on compliance.

Consumers today are understandably very worried about the security of their personal information held by large corporations, including credit bureaus. Some background may be helpful in understanding the benefits of the system, the legal protections, and, I think most importantly, the ways in which consumers can personally manage their financial information.

Our consumer reporting industry evolved over many years in order to meet the needs of banks and commerce so that companies could provide to consumers the products and services they want and need. In the late 19th century, creditors came together to share customer payment information. These voluntary information exchanges then became credit bureaus.

Today, there are four principal credit reporting agencies, but there are also consumer reporting agencies that deal in information other than credit. These deal in information relating to medical payments, landlord/tenant experience, check-writing histories, employment, and insurance claims. Each kind of consumer reporting agency developed because industry members agreed to report their information voluntarily to a centralized system in order to serve the respective needs.

Consumer reporting agencies today maintain large databases on consumers, including personal identifying and sensitive financial information. By engaging in credit transactions, consumers create their credit histories at credit reporting agencies. Consumers don't specifically opt in to having this data maintained and used, but they benefit from the totality of credit reporting agencies' information when lenders use it to verify their identity as well as determine their eligibility for credit.

Despite the clear benefits of the system, the disclosure and use of information in these databases pose risks to consumers. Congress has enacted laws to protect consumers' sensitive information while also assuring that the data is available to meet the needs of commerce. My written statement summarizes these laws, and, believe me, they are extensive.

In addition, Federal and State officials oversee the collection, use, and security of consumers' non-public data through bank supervision and legal enforcement. We may focus on big data when there is a security breach, but companies holding consumers' personal data work continuously to secure the data by monitoring, detecting, evaluating, and addressing security threats. And there are millions of such threats. They perform this monitoring to comply

with Federal and State laws, but they also do it because the data and the integrity of their data is essential to their business. It is not an area where they cut costs.

Despite best efforts, however, data breaches can and do occur. When measured against the volume of potential data security threats, these breaches are very, very infrequent. But when it is my data that is involved, I am less concerned about whether the system otherwise works so well. I think that is how we all feel.

But I know I can protect myself against inaccurate data and the risk of identity theft. Hereis how:

First, I monitor my credit report information through a credit monitoring service. I check my credit report and review it for any suspicious activity. I accept my bank's offers for my free credit score. I read my credit card billing statement when it arrives, and I notify the card issuer if I don't recognize the charges. I also read my checking account statement and contact the bank if there is check fraud. Like everyone, I lead a busy life, but these simple measures do not take much time, they are free, and they make me feel secure.

I also know what to do if I am worried about being a victim of identity theft. I can place fraud alerts on my credit report at the three largest credit bureaus. I can get a free report if I do so. These alerts reduce the likelihood that someone can misuse my information to open a fraudulent credit account.

I can also block the reporting of credit information that has been the result of identity theft. I can go to credit bureaus' websites to learn how to take these steps and to learn more about how to keep my data secure.

I can also go to the FTC's website for identity privacy and online security. It contains a wealth of useful information about privacy and identity theft. The website will also tell me what to do if I become a victim of identity theft.

In sum, there is a tradeoff between consumers' right to privacy of their personal information and the commercial needs and benefits of that information. Our laws reflect that balance in the tradeoff. But we consumers are not powerless in our ability to monitor and control the accuracy, confidentiality, and security of our information.

Thank you.

[The prepared statement of Ms. Fortney follows:]

STATEMENT OF ANNE P. FORTNEY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON
DIGITAL COMMERCE AND CONSUMER PROTECTION

ON

Securing Consumers' Credit Data in the Age of Digital Commerce

NOVEMBER 1, 2017

Anne P. Fortney
Hudson Cook, LLP
1909 K Street N.W.
4th Floor
Washington, DC 20006

Summary of Prepared Statement

Consumers today are understandably concerned about the security of their personal identifying information and credit data held by large corporations, including credit reporting agencies and financial institutions.

The credit reporting industry has evolved to meet the need for data upon which banks and other creditors base their financial transactions with consumers. Credit reporting data enables creditors to provide consumers have access to credit at an efficient cost, promotes the safety and soundness of the banking system, and protects against fraud and other crime.

Federal law exists to protect the accuracy, confidentiality, and security of this personal data. The Fair Credit Reporting Act protects consumer data by limiting access to certain specified purposes, notifying consumers about the use of their information, and ensuring that credit data is accurate. The FCRA also protects against the risk of identity theft by allowing consumers to place fraud alerts on their credit files and to block the reporting of fraudulent information. The GLBA Privacy Rule limits how consumer data is shared with third parties, requires notice about how the data is used, and provides for an opt-out right for such sharing. The GLBA Safeguards Rule requires financial institutions (defined to include credit reporting agencies) to keep consumer data secure. Federal agencies, such as the CFPB and the FTC, enforce these laws. State laws and enforcement of those laws also protect consumers' financial data through their own versions of the FCRA, data security laws, and laws requiring data breach notification.

Thus, consumers have many tools through the credit reporting industry to manage and protect their nonpublic personal information. Consumers should use the tools at their disposal.

Prepared Statement

Chairman Latta, Congresswoman Schakowsky, and members of the Subcommittee, thank you for the opportunity to appear before the Subcommittee on Digital Commerce and Consumer Protection.

I am the partner emerita with the Hudson Cook law firm. Our firm specializes in consumer financial services; my practice involved primarily issues arising under consumer protection laws, including the Fair Credit Reporting Act (FCRA),[1] the Gramm-Leach-Bliley Act (GLBA) rules on consumer data privacy and information safeguards,[2] and similar laws. My experience with these laws included service as Associate Director for Credit Practices at the Federal Trade Commission (FTC), as in-house counsel at a retail creditor, and as a practitioner counseling clients on compliance. I also served as a consultant and an expert witness in litigation involving these consumer protection laws.[3] My career involved more than 40 years' experience with the operation of the consumer reporting industry and the use of consumer report and other nonpublic personal information by creditors and others in the consumer financial services industry.

Because of my extensive background and experience, I was particularly pleased to receive this Subcommittee's invitation to testify at this hearing on securing consumers' credit data in the age of digital commerce. Recent media reports and conversations with friends lead me to believe that consumers are understandably concerned about the security of their personal identifying information and credit data held by large corporations, including credit reporting agencies and financial institutions. At the same time, many consumers appear to lack sufficient information about the existing laws designed to protect the accuracy, confidentiality, and security of this

---

1 15 U.S.C. §§ 1681 *et seq.*
2 15 U.S.C. § 6801; GLBA § 501; 16 C.F.R. Parts 313, 314.
3 A detailed description of my background and experience is attached to this statement.

personal data. In addition, consumers may not know about the ways they can personally manage their financial data at credit reporting agencies.

I begin with a brief overview of the evolution and operation of the credit reporting industry in this country. I also discuss the corresponding evolution in the laws that govern this data and other nonpublic consumer financial data and in federal oversight of the industry. I explain how consumers can manage the accuracy and security of their nonpublic personal information, including credit report data. I conclude with suggestions for improving consumers' access to the benefits of the credit reporting industry.

I. Brief History of the Credit Reporting Industry

The credit reporting industry began with the population growth of towns and cities around this country in the late 19th century and with a corresponding growth in the number of customers at banks and retail establishments. Banks and merchants began exchanging information about their customers' behavior in repaying bank loans and merchants' store credit. These information exchanges became formalized in the collection and reporting of this information by trade associations or centralized bureaus. Over time these reporting agencies expanded to serve larger geographic areas, and the American credit reporting industry became increasingly concentrated in fewer companies serving certain regions of the country. Today, there are four principal consumer reporting agencies: Equifax, Experian, Trans Union, and Innovis. Thus, the credit reporting industry evolved to meet the need for data upon which banks and other creditors base their financial transactions with consumers.

The value of credit reporting data depends on the free collection of the data, and the value is greatest when both positive and negative data are included. While consumers do not choose for their data to be in credit reporting agencies, their participation in the consumer financial services

industry results in that data being available for creditors' use in providing credit and other financial products to them and to millions of other consumers.[4] The large data sets of consumers' credit information enables creditors to evaluate credit applicants relative risk and to provide products and services that meet individual consumers' needs. These data sets also provide the factual basis for credit scoring systems. Our consumer financial services industry is entirely dependent upon credit reporting agencies' data.

Moreover, consumers do not select the information collected and maintained by consumer reporting agencies. If they could so, consumers could remove negative, but accurate data.[5] Then, the entire data set would not reflect consumers' true credit risk and would be much less valuable in creditors' lending decisions. Lenders would need to compensate for the incomplete data by assuming less risk in extending credit, and would do so by stricter credit eligibility standards or higher interest rates and fees, or both.

The comprehensive consumer reporting network is an essential element of our consumer credit system, enabling creditors to make credit granting decisions quickly, accurately and efficiently. The benefits of this network include greater competition among creditors, lower credit costs for consumers and enhanced access to credit. The public also benefits when insurers, employers, landlords, merchants, banks, and others use the information to determine a consumer's eligibility for insurance, employment, a government license or for some other business transaction with the consumer (such as to cash a check or rent an apartment). [6]

---

[4] I discuss below how consumers can prevent or restrict the disclosure of their credit file information under certain circumstances.

[5] Consumers sometimes try to have negative, accurate information removed from their files at consumer reporting agencies by using the services of credit repair organizations ("CROs"). These CROs rarely fulfill their promises to remove this data, but to the extent that they succeed through abuse of the FCRA dispute system, they undermine the validity of the credit report data and jeopardize the safety and security of the consumer financial services industry.

[6] *See also* World Bank Credit Reporting Principles report Executive Summary, *available at* http://documents.worldbank.org/curated/en/662161468147557554/pdf/70193-2014-CR-General-Principles-Web-

Credit reporting agency information is also essential for creditors in processing an application for credit. In addition to use in evaluating the creditworthiness of a consumer, creditors must use the credit report information in order to comply with federal laws and regulations.

The Financial Crimes Enforcement Network, FinCEN, requires various players in the financial markets, including banks and credit unions, to 'know your customer,' meaning that they are required to verify the identity of each customer to the extent reasonable and practicable.[7] This requirement is important for safety and soundness, as well as anti-money laundering, reasons. These entities must obtain certain specified items of information and may do so by verifying identity information against information received from a consumer reporting agency.[8] Additionally, The federal banking regulators, through the Federal Financial Institutions Examination Council, the FFIEC, expect financial institutions to implement multifactor authentication controls to mitigate identity risks for certain high-risk transactions.[9] Financial institutions often use consumer report information to ask "out of wallet" questions to customers as part of multifactor authentication. Furthermore, the FFIEC and the banking regulators expect financial institutions to implement a Bank Secrecy Act/Anti-Money Laundering compliance program to ward against money laundering and terrorist financing.[10] Consumer report information is essential to effective customer due diligence.

Ready.pdf, which summarizes the benefits of credit reporting to a country's economy: "Credit reporting addresses a fundamental problem of credit markets: asymmetric information between borrowers and lenders, which may lead to adverse selection, credit rationing, and moral hazard problems." "In competitive markets, the benefits of credit reporting activities are passed on to borrowers in the form of a lower cost of capital, which has a positive influence on productive investment spending."

7 31 C.F.R. § 1020.220(a)(2).

8 31 C.F.R. § 1020.220(a)(2)(ii)(B)(1).

9 Authentication in an Internet Banking Environment (2005 Guidance), *available at* https://www.ffiec.gov/pdf/authentication_guidance.pdf; Supplement to Authentication in an Internet Banking Environment, *available at* https://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

10 FFIEC BSA/AML Examination Manual, Customer Due Diligence, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm.

The Red Flags Rule, promulgated under the FACTA amendments to the FCRA, requires creditors to implement an identity theft prevention program.[11] The program is required to detect whether there are "red flags" indicating identity theft. Consumer report information forms the basis for important red flags, like if there is a fraud alert or notice of address discrepancy, which are regulated by the FCRA,[12] or if a consumer report indicates a pattern of unusual account activity. Finally, the Truth in Lending Act now requires—after Dodd-Frank—that creditors make a reasonable and good faith determination based on verified and documented information that the consumer has a reasonable ability to repay a mortgage loan.[13] Regulation Z, which implements TILA, requires a creditor to consider a consumer's credit history and outstanding obligations, among other things, in deciding whether to extend credit,[14] verifying those items using third-party records like a credit report.[15]

Our credit reporting industry should not, and today does not, operate without regard for consumers' interest in the accuracy, transparency, confidentiality, and security of their consumer report data. As the credit reporting industry evolved, it became increasingly clear that industry standards were needed to protect consumers. The industry trade association, Associated Credit Bureaus,[16] developed such standards. Those became the foundation of the Fair Credit Reporting Act of 1970.

---

[11] 16 C.F.R. § 681.1(d)(1).
[12] FCRA §§ 605(h), 605A, 605B; 15 U.S.C. §§ 1681c(h), 1681c-1, 1681c-2.
[13] 15 U.S.C. § 1639(c).
[14] 12 C.F.R. § 1026.43(c)(2).
[15] 12 C.F.R. § 1026.43(c)(3).
[16] Associated Credit Bureaus was the successor to the Consumer Data Industry Association.

II. Fair Credit Reporting Act

A. Overview

When Congress enacted the Fair Credit Reporting Act, it recognized that the safety and soundness of the financial services industry depends on the availability of consumer credit report information.[17] Congress also found that consumers need legal protection with respect to the accuracy, fairness and confidentiality of the information:

> It is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information . . ..[18]

This balance of the industry's need for consumer reporting information and consumers' rights is at the foundation of the FCRA. The industry does not have an absolute right to disseminate and use the information, and consumers do not have an absolute right to the privacy of the data. There have been two significant sets of amendments to the FCRA (in 1996 and 2003), and today the Act balances the competing needs of industry with consumers' rights with respect to confidentiality, accuracy, transparency and access, data security and identity theft protection. In the process, the FCRA provides the legal framework for the efficient, fair, and cost-effective credit marketplace upon which our economy depends.

B. Confidentiality and Security

The FCRA's protections for the confidentiality of consumer report data also protect the data from unauthorized access.

The FCRA requires a consumer reporting agency to:

---

[17] FCRA § 602(a); 15 U.S.C. § 1681(a).
[18] FCRA § 602(b); 15 U.S.C. § 1681(b).

- Maintain reasonable procedures to limit the release consumer reports only to persons having a statutorily defined "permissible purpose" to obtain it.[19]
- Require that prospective users of consumer report information identify themselves, certify the purpose for which the information is sought and certify that the information will be used for no other purpose.[20]
- Maintain reasonable procedures to verify the identity of the person seeking the information and the existence of a permissible purpose.[21]
- Maintain reasonable procedures to avoid releasing consumer information to any person not legally authorized to have it or for an unauthorized purpose.[22]
- Keep accurate records of every person who receives a report on a particular consumer and disclose to the consumer on request the identities of these recipients.[23]

C. Transparency and access

Consumers regularly receive notice about the use of credit reports:

- Applications for credit usually include a notice that the lender is will consult with and report data to a consumer reporting agency. These notices typically appear in bold print immediately above the borrower's signature space.
- The FCRA requires lenders to notify consumers if they furnish to a consumer reporting agency, including instances when they furnish negative data.[24] This notice is typically included in every monthly billing statement sent to the consumer.
- Financial institutions that share data with third parties, including consumer reporting agencies, are required to provide privacy notices with detailed information on the covered entity's practices with respect to the sharing of this information.[25] These statements typically inform consumers that information is shared with consumer reporting agencies. These privacy notices are provided when the individual becomes a client of the covered institution and may be sent annually to customers.[26]
- The user of a consumer report that takes "adverse action" against a consumer based in whole or part on information in a consumer report must inform the consumer of the action and of the consumer's rights under the law, including the right to receive a free credit report.[27]

---

[19] FCRA §§ 604(a), 607(a); 15 U.S.C. §§ 1681b(a), 1681e(a).
[20] FCRA § 607(a); 15 U.S.C. § 1681e(a).
[21] *Id.*
[22] *Id.*
[23] FCRA § 609(a)(3); 15 U.S.C. § 1681g(a)(3).
[24] GLBA § 502(a); 15 U.S.C. § 1681s-2(a).
[25] 15 U.S.C. § 6802(a).
[26] 16 C.F.R. §§ 313.4, 313.5.
[27] FCRA § 615(a); 15 U.S.C. § 1681m(a).

- When the user of a credit report engages in "risk-based pricing" using credit report information, the user must give the consumer a risk based pricing notice or a credit score disclosure.[28] These notices include the consumer's own credit score and the key factors that have negatively affected the score (such as the number of delinquencies, or the existence of a bankruptcy, etc.). They also educate consumers about credit scoring and explain how the consumer's credit score compares to those of other consumers.[29]
- Through the credit score initiative of the Consumer Financial Protection Bureau ("CFPB"), creditors regularly provide their customers with free credit score disclosures.

In addition, under the FCRA, consumers have the right to see all the information about them in a consumer reporting agency's files at any time and may receive a free credit report annually from each of the credit reporting agencies that operate on a nationwide basis.[30] In addition, consumers are entitled to a free credit report upon the consumer's request:

- When the credit report is used in whole or in part by the user in making an "adverse action" determination with respect to the consumer;[31]
- When a notification from a debt collection agency affiliated with the consumer reporting agency stating that the consumer's credit rating may be or has been adversely affected;[32] and
- Annually, if the consumer certifies in writing that the consumer –
    - is unemployed and intends to apply for employment in the 60-day period beginning on the date on which the certification is made;
    - is a recipient of public welfare assistance; or
    - has reason to believe that the file on the consumer at the agency contains inaccurate information due to fraud.[33]

---

28 12 C.F.R. § 1022.72.
29 12 C.F.R. § 1022.73.
30 FCRA § 612(a); 15 U.S.C. § 1681j(a).
31 FCRA § 612(b); 15 U.S.C. § 1681j(b).
32 *Id.*
33 FCRA § 612(c); 15 U.S.C. § 1681j(c).

A consumer may also receive a free credit report from a nationwide consumer reporting agency when the consumer places a fraud alert on his or her credit file at the consumer reporting agency,[34] as further explained below.

Thus, Congressional policy has made the transparency of credit reports and credit scores a top priority. An estimated 120 million credit-score disclosures are distributed each year to consumers when they apply for a mortgage, are denied credit or are offered less favorable credit terms by a lender. In addition, CFPB estimates that roughly 50 million credit scores are delivered to consumers on their monthly billing statements through the scores on statements initiative.[35]

D. Accuracy and Consumer Dispute Resolution

A consumer reporting agency must maintain reasonable procedures to assure the maximum possible accuracy of the consumer report information before releasing it.[36] In addition, consumers have the right to dispute inaccurate information free of charge. [37] If the consumer reporting agency cannot verify the accuracy of the information, it must be corrected or deleted, and the agency must report the results of its determination to the other two consumer reporting agencies.[38] If the dispute is not resolved to the consumer's satisfaction, consumer reporting agencies must allow consumers to include in their file a brief statement that the consumer believes the information to be incomplete or inaccurate.[39]

---

[34] FCRA § 612(d); 15 U.S.C. § 1681j(d).

[35] CONSUMER FINANCIAL PROTECTION BUREAU, "CFPB Reports That More Than 50 Million Credit Card Consumers Have Access to Free Credit Scores" (February 19, 2015), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-reports-that-more-than-50-million-credit-card-consumers-have-access-to-free-credit-scores/.

[36] FCRA § 607(b); 15 U.S.C. § 1681e(b).

[37] FCRA §§ 611, 623; 15 U.S.C. §§ 1681i, 1681s-2.

[38] FCRA § 611(a)(5); 15 U.S.C. § 1681i(a)(5).

[39] FCRA § 611(b); 15 U.S.C. § 1681i(b).

II. Other Data Security and Privacy Laws

Consumer data held by consumer reporting agencies is also subject to regulation and protection under other privacy and data security laws. The following is a brief summary of the federal and state regulation of consumers' privacy and data security.

A. GLBA Privacy Rule

The GLBA Privacy Rule seeks to protect consumer financial privacy by providing consumers with notice and choice. Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties.[40] The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions because they engage in certain "financial activities."[41] Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they don't want their information shared with certain nonaffiliated third parties.[42] In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information.[43]

The FTC, the federal banking agencies, other federal regulatory authorities such as the Securities and Exchange Commission, and state insurance authorities enforce the GLBA Privacy Rule.[44] Each agency has issued substantially similar rules implementing GLB's privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance

---

40 16 C.F.R. § 313.1(a)(2)
41 16 C.F.R. § 313.3(k).
42 16 C.F.R. § 313.6.
43 16 C.F.R. §§ 313.10, 313.11.
44 15 U.S.C. § 6805.

providers.[45] The FTC has jurisdiction over any financial institution or other person not regulated by other government agencies.[46]

The FTC may bring enforcement actions for violations of the Privacy Rule. The FTC can bring actions to enforce the Privacy Rule in federal district court, where it may seek the full scope of injunctive and ancillary equitable relief.[47]

B. GLBA Safeguards Rule

The GLBA also requires "financial institutions" to ensure the security and confidentiality of the information they maintain on consumers through appropriate safeguards.[48] As with the Privacy Rule, the definition of "financial institution" includes many businesses beyond traditional banks – it applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services.[49] This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and professional tax preparers. The GLBA security and confidentiality requirements also apply to companies like credit reporting agencies and payment processors that receive information about the customers of other financial institutions. In addition to developing their own safeguards, financial institutions covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.[50]

The provisions are enforced through the Interagency Guidance issued by the Federal Reserve and the other banking prudential regulators,[51] and through the Safeguards Rule issued by

---

45 15 U.S.C. § 6805(a)(6).
46 15 U.S.C. § 46.
47 15 U.S.C. § 45.
48 16 C.F.R. § 314.3.
49 16 C.F.R. § 314.2(a).
50 16 C.F.R. § 314.4.
51 66 Fed. Reg. 8616 (Feb. 1, 2001).

the FTC.[52] Financial institutions are required to develop an information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure their contracts require them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[53]

The requirements are designed to be flexible. Financial institutions should implement safeguards appropriate to their own circumstances. Financial institutions must consider and address any unique risks raised by their business operations, such as the use and location of service providers and data storage facilities.[54]

C. FTC Regulation of Data Security

In addition to enforcing the FCRA and the GLBA privacy and safeguards rule, the FTC uses its enforcement authority under Section 5 of the FTC Act to pursue companies that misrepresent their data security practices or that lack adequate data security measures.[55] Since

---

[52] 16 C.F.R. Part 314.

[53] 16 C.F.R. § 314.4.

[54] *See, e.g.*, 12 C.F.R. Part 30, app. B.

[55] Section 5 prohibits unfair or deceptive acts or practices and provides that an act or practice is unfair if the act or practice (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(a) and (n). *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), *available at* https://fas.org/sgp/crs/misc/R43723.pdf.

2001, the FTC has used its authority to bring enforcement action and obtain settlements in approximately 60 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information. [56]

In addition to the identitytheft.gov website, the FTC has a number of resources to help consumers protect their sensitive information and the steps that a consumer may take if their information is the subject of a breach.[57] The FTC's consumer resources include information about online privacy, computer security, malware, and mobile device security.

D. CFPB Enforcement of Unfair, Deceptive or Abusive Acts or Practices ("UDAAP")

The Consumer Financial Protection Act authorizes the CFPB to enforce civil penalties against entities within its jurisdiction that commit UDAAP violations.[58] The CFPB has used this civil penalty authority in the data security context. In an action against a company for allegedly deceiving consumers about its data security and the security of its online payment platform, the CFPB required the company to enact comprehensive data security measures and policies, including a program of risk assessments and audits, to train employees on the company's data security policies and procedures, and on how to protect consumers' sensitive personal information, to fix any security weaknesses found in its web and mobile applications, and securely store and transmit consumer data, and to pay a $100,000 civil money penalty.[59]

---

[56] FEDERAL TRADE COMMISSION, "Prepared Statement of the Federal Trade Commission on Small Business Cybersecurity: Federal Resources and Coordination Before the Committee on Small Business" (March 8, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1174903/p072104_commission_testimony.pdf.

[57] FEDERAL TRADE COMMISSION, "Privacy, Identity & Online Security," *available at* https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

[58] 12 U.S.C. §§ 5536(a)(1)(b), 5565(c).

[59] CONSUMER FINANCIAL PROTECTION BUREAU, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices" (March 2, 2016) *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

Like the FTC, the CFPB has put out resources to help consumer understand the ways in which they can protect themselves from identity theft.[60]

E. State Attorneys General Enforcement of Data Security Laws

Many state laws regulate aspects of data security that impose obligations on consumer reporting agencies. These laws are categorized as follows:

- General data security laws: at least 13 states require businesses that own, license, or maintain personal information to implement and maintain reasonable security procedures and practices and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. The law in Massachusetts includes 30 discrete obligations concerning administrative, technical, and physical safeguards that organizations must satisfy when handling sensitive personal information.
- Social Security Numbers ("SSN") confidentiality laws: The majority of states require organizations to protect the confidentiality of SSNs.
- Data disposal laws: The majority of states have enacted laws requiring secure disposal of sensitive personal information.

F. State Data Breach Notification Laws

Nearly every U.S. State, the District of Columbia, and several U.S. territories, have enacted laws requiring notification to affected individuals in the event of a security breach of personal information. Most of these laws exempt financial institutions that are supervised by prudential banking regulators and subject to the GLBA Interagency Guidance, discussed above. Consumer reporting agencies are not exempt and must comply with the more than four dozen breach notification laws in the event of a breach.

E. Identity Theft Protections

The 2003 amendments to the FCRA added new protections for consumers against identity theft and other unauthorized access to and use of their data at consumer reporting agencies. These

---

[60] CONSUMER FINANCIAL PROTECTION BUREAU, "Identity Theft Protection Following the Equifax Data Breach" (September 9, 2017) *available at* https://www.consumerfinance.gov/about-us/blog/identity-theft-protection-following-equifax-data-breach/.

protections include the placement of fraud alerts and blocking the reporting of credit report data that reflects identity theft.[61]

1. Fraud Alerts

Under the FCRA, when consumers believe that they may be at risk of fraud or identity theft, they may place fraud alerts on their credit reporting files. There are two kinds of alerts: initial fraud alerts and extended fraud alerts.

A consumer may place an initial alert at no charge by phone, in writing or via the website of any one of the three nationwide credit reporting agencies, and the fraud alert is automatically shared with the other two agencies. An initial fraud alert lasts for 90 days and is renewable upon the consumer's request. When requesting an initial fraud alert, the consumer also may request one free credit report. When a fraud alert is on a consumer's credit file, creditors 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 an existing line of credit.[62]

An extended alert is available for consumers who have become victims of identity theft, but still wish and expect to be credit active. The FCRA allows for a consumer to place an extended alert on the consumer file at no charge for seven years by presenting a copy of a law enforcement report or an FTC identity theft report, which is available at www.identitytheft.gov. Similar to the initial fraud alert, an extended fraud alert filed with one bureau is automatically shared with the other two consumer reporting agencies. However, in contrast to the initial fraud alert, an extended alert requires lenders to actually contact the consumer before extending a new line of credit, increasing a line of credit or issuing a new or replacement card. A consumer can receive two additional free credit reports from each of the three consumer reporting agencies within twelve

---

[61] FCRA §§ 605A, 605B; 15 U.S.C. §§ 1681c-1, 1681c-2.
[62] FCRA § 605A(a); 15 U.S.C. § 1681c-2(a).

months of placing the extended alert. In addition, the consumer's name is taken off marketing lists for prescreened credit offers for five years.[63]

2. Credit Report Tradeline Blocking

When a consumer observes information in her credit file that is the result of identity theft, she can require the consumer reporting agency to block the reporting of that information. The consumer must: provide appropriate proof of identification and a copy of an identity theft report, tell the consumer reporting agency what information is to be blocked; and provide a statement that the information does not relate to the consumer's transaction. Once the consumer reporting agency receives an appropriate tradeline block information, the agency must stop reporting the information and must inform the furnisher.[64]

F. State Versions of the FCRA and Security Freeze Laws

Many states have enacted their versions of the FCRA in order to further protect consumers under state law.[65] In addition, every State has enacted laws permitting consumers to place a security freeze on the consumer file at each credit reporting agencies. Security freezes may protect consumers from identity theft and may also be used by consumers who do not plan to be credit active. When a freeze is in place, the consumer's file cannot be accessed for purposes involving extension of new or existing credit unless the consumer contacts the credit bureau to lift the freeze.

---

[63] FCRA § 605A(b); 15 U.S.C. § 1681c-1(b). The FCRA also permits individuals on active duty to place active duty alerts. § 605A(c); 15 U.S.C. § 1681c-1(c).

[64] FCRA § 605B; 15 U.S.C. § 1681c-2.

[65] *See, e.g.*, Ariz. Rev. Stat. §§ 44-1691 *et seq.*; Cal. Civ. Code §§ 1785.1 *et seq.*; Conn. Gen. Stat. §§ 36a-695 *et seq.*; Kan. Stat. Ann. §§ 50-701 *et seq.*; LSA-R.S. 9:3571 *et seq.*; Md. Com. Code §§ 14-1201 *et seq.*; Ma. Ann. Laws Ch. 93, §§ 50 *et seq.*; Mont. Code Ann. §§ 31-3-101 *et seq.*; Nev. Stat. §§ 598C.010 *et seq.*; N.H. Rev. Stat. §§ 359-B *et seq.*; N.J. Stat. Ann. §§ 56:11-29 *et seq.*; N.M. Stat. Ann. §§ 56-3-1 *et seq.*; N.Y. Gen. Bus. §§ 380 *et seq.*; Tex. Bus. & Com. Code Ann. §§ 20.01 *et seq.*; 9 V.S.A. §§ 2480a *et seq.*; Wash. Rev. Code Ann. §§ 19.182.005 *et seq.*

Some states further prohibit releasing a frozen file for purposes involving insurance, rental housing, employment, telephone services, utilities, or government benefits.[66]

A freeze remains on the file until the consumer lifts or removes the freeze using a PIN provided at the time of placement. State law permits a fee for placing, lifting and replacing a freeze. These fees are typically between $5-$10 per transaction to impose or lift the freeze, unless the consumer is an identity theft victim.[67]

III. Consumers' Rights and Control Over Personal Data and Consumer Reports

It should now be clear that consumers' personal data at consumer reporting agencies is protected by a comprehensive regulatory scheme at the federal and state level. These laws also provide notice to consumers about the use and their access to consumer report information. Consumers can protect themselves in the following ways:

- Request copies of their credit report from the nationwide consumer reporting agencies.
- Review the contents of the reports for apparent inaccuracies or suspicious activity.
- Dispute any information that the consumer believes to be inaccurate or incomplete with the consumer reporting agency and/or the creditors that provided the information to the agency.
- Read their credit card statements and immediately notify the card issuers of any errors or other billing disputes.
- Check their credit scores when their credit card companies offer that information.
- Read the privacy notices that financial institutions must send if they share the consumers' nonpublic personal information with affiliates for marketing purposes or with nonaffiliated third parties. Opt-out of the disclosure of information when the consumer can restrict its being shared with others.

---

[66] *See, e.g.*, Cal. Civ. Code § 1785.11.2(l); Conn. Gen. Stat. Ann. § 36a-701a(g); Idaho Code Ann. § 28-52-105; La. Stat. Ann. § 9-3571.1(V); Me. Rev. Stat. Tit. 10 § 1310(1)(M); Mich. Comp. Laws Ann. § 445.2513; Minn. Stat. Ann. § 13C.016 subd. 6; Miss. Code Ann. § 75-24-209; Mo. Ann. Stat. § 407.1382(4); Mont. Code Ann. § 30-14-1734(1); Nev. Rev. Stat. Ann. § 598C.380; N.J. Stat. Ann. § 56:11-46(l); N.Y. Gen. Bus. Law § 380-t(m); Tex. Bus. & Com. Code Ann. § 20.038; Utah Code Ann. § 13-45-203; Wash. Rev. Code Ann. § 19.182.170(14); Wyo. Stat. Ann. § 40-12-505.

[67] For those consumers who are not identity theft victims, most states permit one or all of these fees to be charged. *See, e.g.*, Ala. Code § 8-35-2; Cal. Civ. Code § 1785.11.2(m); D.C. Code Ann. § 28-3862; Ga. Code Ann. § 10-1-914; Kan. Stat. Ann. § 50-723(j); Mo. Ann. Stat. § 407.1382(2); N.H. Rev. Stat. Ann. § 359-B:24(I)(b); Ten. Code Ann. § 47-18-2108; and 9 V.S.A. § 248oh(a).

- Read prescreening notices and opt-out of receiving prescreened solicitations if the consumer chooses to do so.[68]

In addition, if consumers are concerned that their credit report data has been hacked or otherwise disclosed to an unauthorized person, consumers can take the following steps to protect themselves from the risk of identity theft or other misuse of the data:

- Place an initial fraud alert, an extended fraud alert, or an active duty alert on the consumer's file at a nationwide consumer reporting agency and obtain a free credit report.
- Enroll in a credit monitoring service. When consumers' sensitive identifying information or credit report information has been involved in a data security breach at a financial institution or credit reporting agency, consumers are usually offered credit monitoring services at no charge for a certain period of time.
- Obtain a security freeze on the consumer's file at the consumer reporting agency. While the freeze may prevent third-party access to the consumer's file, the consumer can obtain credit only by taking the step of contacting the consumer reporting agency in advance of applying for credit and arranging for the freeze to be lifted. For this reason, consumers who are credit active and/or are seeking employment, housing or utility services may find that having a freeze, and then needing to lift it, significantly slows transactions. Presuming the consumer has kept the PIN, most state laws require the consumer reporting agency to lift the freeze within three days of being contacted. Many times, a freeze can be lifted more quickly, but it is not always instantaneous. For example, if the consumer does not have his or her PIN, then the consumer reporting agency must authenticate and verify the consumer, which may take several days, especially if accomplished through the postal system. In addition, because of the unique characteristics of each consumer reporting agencies' system and the fact that a unique PIN must be provided to each consumer from each bureau, security freezes cannot be shared across bureaus and the consumer must place the security at each bureau independently. Thus, a security freeze may delay the consumer's application for credit. So, this option may be the consumer's choice as long as the consumer accepts the consequences of the freeze.

[68] Pre-screened offers of credit and insurance must include a notice informing the consumer that he has been selected to receive the offer because of prescreening. The notice must also tell the consumer how to opt-out of receiving pre-screened solicitations. FCRA § 604(c); 15 U.S.C. § 1681b(c); 16 C.F.R. Part 642.

IV. Conclusion

The laws governing the consumer reporting industry reflect the balance between (a) creditors' need for credit history data in providing credit products and services to consumers in a fair and efficient manner and (b) consumers' needs for privacy, accuracy, and security of the data. As a result, the regulatory controls in place ensure that consumer information is accurate and kept confidential and secure, while also ensuring the availability of the data upon which the consumer financial services industry depends.

These laws also give consumers the tools necessary to ensure the accuracy and completeness of the data, to protect their personal information for its intended use, and to guard against identity theft.

Mr. LATTA. Well, thank you very much for your testimony today.

And, again, we appreciate all of our witnesses for being with us today.

And that will conclude the witnesses, and we will start with our Members' questioning. And I will start with my 5 minutes.

Mr. Creighton, if I could start with you, considering the size and scope of the Equifax breach, consumers are confused and rightfully skeptical about what they should be doing to protect themselves.

Could you briefly—and briefly because I have limited time—what should we tell our constituents about how the credit reporting industry is securing your sensitive data? And, trust me, we are all hearing it from our constituents from phone calls when we are back home.

So thank you very much for being here.

Mr. CREIGHTON. Sure. And I hear it too. Obviously, this impacts us, everyone here on the panel, as much as it impacts you.

What is the industry doing to protect our data? The same thing every company that has sensitive information is doing: They are monitoring their systems. They are learning from every breach that happens, not only in our industry but across the economy. We are fighting this war on a daily basis. We are getting attacked nonstop, from nation-states, as one of the other witnesses was mentioning, from criminals, and from many others.

What do we do? We monitor. We test our system. We try to do data minimization and encryption, inside and while the data is in transit, to make sure that if, in fact, somebody is in the system the information is not usable if they are in there and to try to keep them out of the system in the first place.

Taking care of consumers' sensitive personal information is the most important thing that we do. In this case, we failed. But it is still the entire industry's number-one priority.

Mr. LATTA. Thank you very much.

Mr. Norton, Equifax is subject to Federal data security standards. Other industries are subject to Federal and State security standards. However, breaches continue in all the sectors.

When companies are evaluating how to protect individuals' data from cyber criminals or nation-states, are there best practices to follow? And, most importantly, how effective are the regulations that are out there in policing companies' cybersecurity practices today?

Mr. NORTON. Well, I think it is obvious by the number of attacks we have seen every day, every week, every year that we are not doing enough. So I think that is pretty clear, that, you know, the larger corporations, whether it is Equifax, Home Depot, or Target, they have all been exposed and they have all been attacked because they all are targets because they have a large amount of information on their systems.

I think partnerships through places like Department of Homeland Security, Department of Commerce are important to establish. I think real-time information needs to be exchanged a lot faster than it is right know. I think we need to almost indoctrinate some of the business partners with the Federal Government in terms of allowing them to get some of this sensitive information and create

that culture that I don't think really exists, you know, at a lot of C-suites right now.

Mr. LATTA. Let me ask you about what you just said. OK, exchanging that data in real time, that real-time data, how would you describe that, and how should that be done?

Mr. NORTON. Well, I think that you need, you know, certainly, somebody that is at a senior level within—a CEO—so let's use States, for example. After the 9/11 attacks, a lot of Governors stood up homeland security apparatuses at the State level and they had homeland security advisers, and I think you need a similar model at the CEO level, where the CEO has a cybersecurity—not just an adviser but somebody that is at a senior level that can be in the meeting not once a month, not every 6 months, not every quarter, but every day, and they can get briefed every day on these threats.

Any company that has large amounts of personal information, like we were talking about earlier, like Equifax, or large amounts of other types of IP, you know, for example, companies that have, you know, high-end, valuable assets that might be for sale, again, would be something that would be attacked.

So I think all these things need to be considered and need to be part of that exchange in terms of the day-to-day threat information. And if DHS or other agencies, you know, need more funding or they need to continue to stand up, then that is an area that I think the subcommittee could definitely support.

Mr. LATTA. Thank you.

Ms. Fortney, given your experience at the FTC and in your legal practice, what potential consequences do you see for Equifax given the regulatory environment? And, again, what laws and regulations are at play in this situation?

Ms. FORTNEY. The first thing we need to do is find out exactly what happened. And the FTC has announced—they took the extraordinary step to announce that they were conducting what is usually a non-public investigation.

We don't know exactly what has happened. The fact that there has been a security breach in general doesn't mean that there is a violation of the law. From what we have read—and all I know is what I have read in the press—Equifax did not take appropriate measures to prevent the breach.

The Fair Credit Reporting Act, if there is any credit reporting information that is involved, would come into play. There are civil penalties, as well as the FTC's authority to prevent future violations.

The Gramm-Leach-Bliley rules also require Equifax to safeguard the data on consumers that it holds, and there can be penalties there as well. I understand that there is some confusion in terms of whether a violation of the rule itself would result in penalties, but I think the FTC also has authority under other laws.

In addition, the FTC has taken the position that their authority to address unfair, deceptive acts or practices can come into play when there is a serious security breach.

Mr. LATTA. Thank you very much.

My time has expired, and the Chair recognizes the ranking member of the subcommittee, the gentlelady from Illinois, for 5 minutes.

Ms. SCHAKOWSKY. Thank you.

Mr. Schneier, you recommended that Congress move forward with legislative proposals to make a credit freeze the default, effectively blocking access to consumer credit reports except when the consumer permits access for the specific purpose.

You believe this step would protect consumers' privacy and make consumer information more secure. Is that correct?

Mr. SCHNEIER. I think it will prevent the breaches. It is not going to do anything to make Equifax's databases more secure. It is not going to do anything to make our data less vulnerable, but it will make it less useful. And that, I think, is something that is real important.

Ms. SCHAKOWSKY. Well, let me ask you this. You said that we, the public, are not the customer of Equifax or the data reporting agencies. We are, in the sense that—I am sort of galled by the idea that I have to pay for the credit report. Actually, I did also go for the one free, and somehow I must have pushed a button that, then, $10 a month was charged in the future. I finally called them and said, "How did that happen?" You know, I don't exactly know.

So we do pay a small amount every month. So they still do charge us for our—you know, except for the one free.

Who are, then, the customers? I have gotten a—what do you call it—preapproved credit cards in the mail. I didn't ask for that. I am not seeking a loan. So who are the customers, then, of these CRAs?

Mr. SCHNEIER. The customers are those who want to give you offers. And, certainly, anybody who sent you a preapproved credit card got that data.

And they get data in very different ways. There was something I wrote about, and I don't remember the details, but one lender was asking for people who had defaulted on loans so they can sell them basically fraudulent products. The FTC did slap a fine on them, but those are the sort of things that are happening.

And the way to think of it is that we are not their customers. And they deliberately make it hard—those credit freezes and credit scores, they are deliberately deceptive. To get the free one, you have to navigate a very complex route, and occasionally you get taken. There are a lot of things these companies do——

Ms. SCHAKOWSKY. [Inaudible.] The score, you know?

Mr. SCHNEIER. That is right.

Ms. SCHAKOWSKY. So the score isn't free, in some cases.

Mr. SCHNEIER. That is right. Just the data is, so you can look at it.

Ms. SCHAKOWSKY. Right.

Mr. SCHNEIER. And, in some cases, there are things they can do to make things easier, and they don't. So, for example, if I log into my network at Harvard, this phone will make a noise and will tell me. So if someone else does it, I will know that. And you can get an app from some banks that, if your credit card is used in a physical location you are not, like in California today, you would be alerted. You are not near your card.

And that is sort of a customer-service type of thing. There is no reason in the world why the credit agencies can't do that same thing: When someone wants my credit, I get an alert. You know, retailer I like? Yes. You know, Russian scammy bank? No. I mean, I should be able to do that.

But that is a feature that is not going to be offered to the product. As the product, we are supposed to, you know, shut up and do what we are told. And if you complain, there are going to be difficult avenues and you are going to get scammed.

Ms. SCHAKOWSKY. So I think people need to understand this is not just, I am applying to refinance my mortgage or I want to get a car. This is, my information is now a product that they can sell to others. Is that right?

Mr. SCHNEIER. And it is more than financial information. You have to understand, it is our browsing habits, it is our reading habits, it is the things we do, it is the details of our life.

I mean, you have to assume that that will be purchased by somebody who wants to use it against you. And I think all of our Government officials should be concerned about that. Do we want our browsing habits in the hands of opposition research? Kinda not.

Ms. SCHAKOWSKY. Have we seen any international reaction to this Equifax breach? You talked about the problems that we may incur if our partners around the world think that we can't protect data.

Mr. SCHNEIER. I haven't heard anything about Equifax specifically, but certainly there is agitation in Europe. A lot of these safe harbor agreements are very tenuous. And they are right now protecting American companies to store Europeans' data, but I think we can lose them at any time, especially as Europe is getting much more regulatory. The GDPR is coming, and it is going to be enforced starting in March, and all the U.S. companies are preparing for that.

Ms. SCHAKOWSKY. So there is personal and international consequences for consumers and for business.

Mr. SCHNEIER. I think there is. I worry about how the U.S. will look in the world market if we show that we can't secure the data of Canadians and British and Europeans.

Ms. SCHAKOWSKY. Thank you.

Mr. LATTA. Thank you very much.

The gentlelady yields back, and the Chair now recognizes the gentleman from Mississippi, the vice chairman of the subcommittee, for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman.

And thank you to each of you being here. Particularly, Mr. Norton, I want to thank you. On such short notice, I am sure you had other things you might have preferred to do. But the information that each of you are providing is very important.

Who knows, Mr. Schneier? Maybe we will get back to just writing letters. You know, maybe that is going to be the solution to protect our personal information on some of this.

You know, this is still just an unbelievable event that has raised this to a new level. And, Mr. Creighton, I know that—you know, we can talk about this. When I questioned the former CEO of Equifax, you know, he said, that is the number-one issue, which you restated, which is to protect that personal information, which was done very poorly.

So there are so many issues here, but do all three—and this is for you, Mr. Creighton—do all three major credit reporting agencies

provide the same information to every lender, merchant, et cetera? If not, why is that not the case?

Mr. CREIGHTON. Different bureaus may have different institutions furnishing information into them. When a lender asks for information, they will provide the information that they have, but not every bureau has exactly the same information that every other bureau does.

It is one of the reasons why Fannie Mae and Freddie Mac, for example, require that their lenders collect all three credit reports and merge them into one package, to make sure they are getting full coverage.

Mr. HARPER. So you could request three or four credit reports from different CRAs, and they could have variations based upon that technique.

Mr. CREIGHTON. Well, for example, if you are an auto dealer, a small auto dealer in a particular region, you might only be working with one credit bureau.

Mr. HARPER. Got it.

Now, do credit reporting agencies separate their credit reporting and non-credit reporting activities and businesses?

Mr. CREIGHTON. Yes. This is an important point. The credit file is distinct from any other business that they have. The credit file is governed by the Fair Credit Reporting Act.

And the credit file is only certain kinds of information. It is not the web browsing and all of that other information. What is in the credit file? Who are you? Who are you, personally? Do you exist? That is, you know, basically public information. Do you have any judgments again you, like a bankruptcy? Do you have credit available? With whom do you have that credit available? How much credit do you have? What is your balance? Do you pay on time? Functionally, that is what is in the credit report.

Mr. HARPER. OK. Thank you for that.

And, Mr. Norton, can you talk to us for just a minute and explain a little bit about NIST, the National Institute of Standards and Technology, and their cybersecurity framework and its importance for today's, you know, hearing?

Mr. NORTON. Yes, absolutely. And, you know, NIST several years ago took an important step, providing voluntary guidance for not only Federal agencies and State and local governments but also for the private sector to start to build out a framework to start to talk about, you know, how do you secure the enterprise——

Mr. HARPER. So when did they start this?

Mr. NORTON. I don't know the exact date. I think it was a few years ago.

Mr. HARPER. OK. Was Equifax a voluntary participant in this?

Mr. NORTON. I don't know if they were. I am not sure.

Mr. HARPER. Can you find that out for us and let us know that?

Mr. NORTON. Sure.

Mr. HARPER. And go ahead and explain this a little bit more, the cybersecurity.

Mr. NORTON. But I think to your point that, you know, it was publicly available information, it was something that the Government was, you know, certainly promoting, in terms of this NIST standard, I think that, you know, having these standards are very

important. I think, you know, the threat still, necessarily, hasn't been digested by the private sector. And I think that is part of, you know, a role that the Government could play, in terms of briefing not only on the standards and the voluntary compliance that they should really look at and think about doing but also understanding what are these attacks, why are they a target, not just, you know, the bigger nation-states but the smaller gangs and the different organizations that are out there that, you know, are certainly targeting these things for money, essentially, and to sell this data.

Mr. HARPER. You know, listening to each of your testimonies, you know, I know Mr. Schneier mentioned that, you know, CEOs willing to take a chance, I don't know if that is going to be the case on the Equifax deal. I think it was just pure negligence. Somebody—multiple people dropped the ball on an easy—you know, this was not a complicated fix. And I know we will find out more when FTC gets through with this and we get through with all the investigation that is there. But, you know, constant upgrades of cyber defenses are necessary. They only have to be, you know, correct one time. And, obviously, this, they were in a big way.

So, Mr. Norton, do you believe that security standards will stop the data breaches as we have now?

Mr. NORTON. You know, I think that it is certainly an important part of it. I think that having cybersecurity as a one-person position within a business is not cybersecurity. That is just having one person. I think you need to have a larger enterprise strategy and plan, and it has to flow up from the CEO all the way down to the lowest employee.

If you look at attacks like OPM was mentioned and others, it is really the training is an issue, where all employees need to be trained on cybersecurity. They need to understand exactly what these threats are. Because at your desktop is really the front door of a business, and when you get, you know, a phishing email or a phishing attack and you click on that link, you have just opened the door.

Mr. HARPER. And maybe not giving an $18 million bonus to somebody who totally failed in their number-one responsibility.

I yield back.

Mr. LATTA. Thank you very much.

The gentleman yields back, and the Chair recognizes the gentleman from California for 5 minutes.

Mr. CÁRDENAS. Thank you, Chairman Latta. I appreciate this opportunity for us as Congress to discuss this very, very critical issue that faces hundreds and hundreds of millions of Americans every single day.

In discussions of data breaches and breach legislation, there has been a tendency to focus on financial harms to consumers. Credit reports include a lot of nonfinancial information, and certainly these companies hold a significant amount of personal information outside of the credit report that is not financial.

Mr.—I am sorry if I pronounce your name wrong—"Schneer"?

Mr. SCHNEIER. "Schneier." That is all right. Nobody has gotten it right today.

Mr. CÁRDENAS. OK. "Schneier." OK. Are you concerned about repercussions of a breach beyond financial harms, and if so, can you give us some examples?

Mr. SCHNEIER. So, yes, I think the nonfinancial harms are considerable. I mean, just thinking of the OPM breach would be an example of just nonfinancial data in the hands of the Chinese Government, and that would be a problem. So, depending on who stole the Equifax data—we actually don't know if it was criminals or a government right now—the harms can be considerable.

And the swap between financial and nonfinancial is fuzzy. If you call your bank or your broker or your insurance company and don't remember your account, they are going to ask you a bunch of questions like where did you live, which of these cars do you own. You have all had that experience. That is nonfinancial data, and that is going to be used to authenticate you to a financial institution. So even nonfinancial data has very serious financial ramifications because it is our secondary authenticator.

Mr. CÁRDENAS. So, in some cases, somebody might know the name of our favorite pet.

Mr. SCHNEIER. Favorite pet is actually surprisingly easy. Those secret questions turn out to be very insecure.

And this is, sort of, again, you are looking at this tradeoff in security and convenience. What these companies want—I mean, what the credit card companies want—is for it to be really easy for you to get a new card, so they make that application super-easy. If they made it more secure, made it harder for somebody else to get a card in your name, it would be harder for you to get a card, and the companies don't want that.

So they are making a tradeoff based on their bottom line, not based on your security, to maximize their profits. And that is often ease of use, ease of access, making things easier.

Mr. CÁRDENAS. Can you give us an example of how nonfinancial information can lead to financial harm to an individual that their information has been breached or gotten into the wrong hands?

Mr. SCHNEIER. So I just talked about nonfinancial information being used as a financial authenticator. You can certainly see personal embarrassment leading to all sorts of problems. I mean, lots of instances of that, especially, you know, people who are more marginalized. We see a lot of threats against women based on exposing personal information that is stolen from accounts. And, I mean, that is something that is a real problem and hard to deal with.

I pulled up to—I talked about something Equifax did. It wasn't in my testimony, and I want to mention it, that in 2012 they sold lists of people who were late on their mortgage payments to a discount loan company. That was one of their products. They were fined by the FTC for that. But those are the sorts of practices you see from these companies.

Mr. CÁRDENAS. So companies like Equifax, they have dual or more than one role out there in the world? Or they see themselves as being involved in businesses beyond just holder of information or reporting of our ability to pay, so to speak? They are actually brokering information out there?

Mr. SCHNEIER. If you go out to their website and look under "business products," which is different from the credit stuff, and they ask things that are optimized for restaurants, for the travel industry, for—and I forget the whole list of industries that they are selling data to. That data is nonfinancial data. It is data about us, slicing and dicing us in different categories, so we can be better marketed to.

Mr. CÁRDENAS. So, basically, when an American puts their house up for sale and you see a sign out front, that is pretty cut and dry that you have hired somebody to broker for you, to actually do something for you, something so personal as we are going to sell our home.

But are you telling me that, unbeknownst to a bunch of American citizens, that companies like Equifax are actually having signs out on their personal information and using it and making money off of it, unbeknownst to the average American?

Mr. SCHNEIER. And that is the business model. The data-broker business model is they collect information, either—they will buy it. They will buy it from the Government. You know, States will sell them driver's license information. They will get it from companies. They will get it from wherever they can. They will correlate it. They will make inferences based on it. I mean, we are hearing about how some of that was used to target ads in the last election. And then they will sell that to people who want it.

Mr. CÁRDENAS. OK.

Well, I yield back my time. Thank you, Mr. Chairman.

Mr. LATTA. Thank you very much.

The gentleman yields back, and the Chair now recognizes the chairman emeritus of the full committee, the vice chairman, the gentleman from Texas.

Mr. BARTON. Thank you, Chairman Latta. And I was here at the gavel. I had to go run to a quick meeting, but I appreciate being allowed to ask questions at your hearing.

The current system is not working. I was here for Gramm-Leach-Bliley. I have been on this committee 33 years. We have all these—as the first gentleman said, in your testimony, it is a heavily regulated industry. You are right about that. But when it comes to data breaches, all that is required is disclosure. There is no real penalty. Eventually, if it happens repeatedly at the same institution, the FTC has some authority to impose some fines.

But all these laws that we have passed merely require that you have to inform the customer, the consumer, of how their data may be used, and if it is breached, you have to inform them that it is breached. That is pretty much it. And I don't think that works.

And if you listen to the opening statements on both sides of the aisle this morning, you know, Mr. Pallone's, Chairman Walden's, the chairman, Mr. Latta, they are all pretty strong on condemnation of what is happening. I think that we are going to have to change the law and that we are going to have to do more than require disclosure. I believe we are going to have to, on first offense, allow for some fines to be levied, some real penalties. I would prefer that it be on a per-consumer basis. That may or may not be workable.

So I guess I will go to Ms. Fortney.

Do you agree or disagree that we need to change the law and put some real teeth into what happens when there is a breach?

Ms. FORTNEY. I think the answer depends on whether the problem with Equifax was a systemic problem or whether Equifax was an outlier.

I think that the law currently exists in ways that consumers can be protected. I think the FTC has indicated that they will use their authority, not just under Gramm-Leach-Bliley but also under Section 5 of the Federal Trade Commission Act, to redress consumers who have been harmed by security breaches and by other data practices that are unfair to the consumer.

Mr. BARTON. Do you support that they be allowed to do that at a first offense?

Ms. FORTNEY. The FTC on their website says that they have brought—sorry, their testimony said they have brought 60 cases against companies under Section 5 of the FTC Act based on unfair, deceptive practices involving data and data security.

Mr. BARTON. Mr. Creighton, your testimony, I thought, was thoughtful. I thought it was well done.

My question to you would be, if we did impose or give some authority to levy fines or a reimbursement to each consumer whose data is breached, would that destroy the credit industry as it is today? Or would it, if it was done appropriately and at the appropriate level, would it perhaps strengthen it because it would give them an incentive to really protect consumer data so that we don't have all these breaches?

Mr. CREIGHTON. The incentives already exist for us to protect the data. You know, if you add penalties and everything else, it is not going to change our practices. Our practices are to protect the data today. So, I mean——

Mr. BARTON. Then why do we have thousands of breaches or hundreds of breaches a year?

Mr. CREIGHTON. It is true. Look, in the Government, you have an incentive to protect your data also, and yet we have seen breach after breach after breach, including personal information for, as the chairman said, people in this room, sensitive market-moving information at the Securities and Exchange Commission. We have seen that over and over and again there. Those incentives need to be aligned, I would argue, more directly with where our incentives are, which is to protect the data.

Yes, breaches happen, and every one of them is a problem. But there are different scales of breaches. You know, is a lost cell phone that has some data on it considered a breach that automatically is going to result—or do you have to look at what is the consumer harm?

Mr. BARTON. Well, my time has expired. I will just make this editorial comment. In the Equifax case, people at Equifax knew they had a problem with their system and they didn't do anything to fix it. They didn't do anything to fix it. But if they would have known, if we don't get this fixed, we are going to pay $1,000 per consumer or $100 or maybe even $50, plus some of the things that Ms. Schakowsky and Mr. Pallone were talking about, I believe they would have fixed it or tried to fix it sooner rather than later.

Thank you for your courtesy, Mr. Chairman. I appreciate it.

Mr. LATTA. Well, thank you very much.

The gentleman's time has expired, and the Chair now recognizes the gentlelady from Michigan for 5 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman.

I guess I am sort of, even before I begin, reacting to "if Equifax is an outlier." I have been hacked so many times in the last—the OPM, the Yahoo account, the Equifax, the Target, the Sears, the Home Depot. You can tell I have a lot of credit. But I have also been hacked more than that. I have a permanent—but I also will tell you that I think it is very complicated to put these credits—and you talk about it very easily, and that is what I do want to talk about, is I think it is very complicated for the average consumer, who, by the way, has no idea what is happening.

Mr. Chairman, I thank you for studying this, because I think it is hard for people to get a sense of how much of their information is held by companies, because it is not tangible. People don't understand what you are holding. You can't hold it. You can't touch it. And we really only think about it after it has been stolen or floating around the internet. So when it has been stolen, like someone like me, 10, 15, 20 times, you think about it. But I think young people, in particular, don't understand what information they are giving away or what is out there.

We have spent a lot of time talking about the legal issues faced, but, for me, it comes down to the question, do Americans really know when they are giving their personal information away? Do they know the consequences? And how can we improve transparency?

"Transparency" is a buzzword that we are all talking a lot about right now, but I think there is a shocking lack of transparency when it comes to how consumers' data is used and sold. So I want to talk about that a little more, and I want to talk about who is even holding it.

Mr. Creighton, I was just interested in your organization. The companies you represent possess a huge amount of granular personal information on us. It is collected without ever really asking. And we are all supposed to trust that it is going to be kept safely, just like the Equifax was.

But I couldn't even figure out who is holding my data that is part of you. I know who the Equifax and Experians of the world are, but I couldn't find who your other members are. There is no mention of your member companies on your website, and a Google search turned up nothing. And I went and looked at your 990, and it has only got your board members.

So this is a yes-or-no question, a friendly yes-or-no, but I want to know: Why should the American people trust an organization like yours to keep their information safe if we don't even know who has it and how they are using it?

Mr. CREIGHTON. First of all, thank you for your comments about the website. We are in the process of redoing it, and I think you will see a lot more information when it rolls out later this year.

Mrs. DINGELL. I am a Dr. Google in this committee. I Google a lot.

Mr. CREIGHTON. Good. Well, I think you will be more pleased in the future when you see the website. It has been a priority of mine since I have taken this position.

Our association represents the main large credit bureaus. We also represent a series of specialty and other credit bureaus that hold other kinds of information that specifically work with a particular industry—for example, the mortgage industry.

We also represent a series of background screening companies that are in our association because they are working mainly on public documents, on public files, which are really the basis, the foundation on which the credit report is built.

And so that is the core of our membership, are the bureaus and the special——

Mrs. DINGELL. I really think that—I have a lot more questions for you, but I have a minute left. But I do hope that you will make public who your companies are and why they are collecting it.

And maybe someday somebody could explain—I understand there are other websites that do this too. I do Credit Karma almost every other day. It is free. Why should the American consumer, my other colleagues on both sides, have to pay for their own credit data when you can go to a site like Credit Karma or others—I don't want to—you know, there are other sites out there. But I think we should look at how people have free access.

But I want to go to Mr. Schneier in the very short time that I have left.

Mr. Schneier, do you think the American consumers can take proactive steps to protect their data, financial or otherwise, if they don't even know who owns it?

Mr. SCHNEIER. There is "can," and there is "can."

So Ms. Fortney gave a really nice list of "here are all the things that you could do to protect yourself." And I am listening to that list, and I am thinking, no way in the world can I go home at Thanksgiving and tell my relatives—because they are going to be a lot harder than you are—that they should do all of that. I can't expect people to become experts in this, to take the time.

And it is not just we don't know who has it; it is that it is being made deliberately hard to figure it out, to take these steps. So, no, I don't.

Mrs. DINGELL. Do you think that we should find a simpler way to tell consumers who is collecting their data, what kind of data they have, and take these privacy notices—which, actually, somebody read the other day, and we found some—and make it in simple language, a couple sentences?

Mr. SCHNEIER. More transparency and more control cannot hurt.

Mrs. DINGELL. Thank you.

Mr. LATTA. Thank you very much.

The gentlelady's time has expired, and the Chair now recognizes the chairman of the Health Subcommittee of Energy and Commerce, the gentleman from Texas, for 5 minutes.

Mr. BURGESS. Thank you, Mr. Chairman.

And I can't help but observe, I feel like this is Groundhog Day. The previous Congress, I was chairman of this subcommittee, and for 2 years we worked on data breach notification. And we actually got a bill through the subcommittee and the full committee. It

never saw time on the floor. It did become controversial before it passed out of the full committee. And I can't help but think, had those requirements been in place, at least the length of time between discovery of a breach and notification of the person who was breached, I think that would have been helpful.

But I am always struck when we have these discussions—and I realize this is not a law enforcement panel in front of us, but do any of you know, is anybody trying to catch the thief here, or the thieves?

Mr. CREIGHTON. Thank you for asking that.

We have to, as a society, come to terms with the fact that we have people attacking our systems every day. If this were a physical bank and there were 200 North Koreans who were storming in and taking money out of the accounts, there would be a national response. At what point are companies able to compete against nation-states who are attacking our systems?

I don't know that this breach was a nation-state attack. I don't know one way or the other. But at what point are American companies expected to fight back against countries that are attacking them?

Mr. BURGESS. Well, then that brings up—and this is really a question for anyone on the panel. I am also concerned—I mean, Equifax obviously did not cover themselves in glory in this story, but in some ways they are a victim too. Their business was damaged by someone who came in—it wasn't Frank and Jesse James storming the Northfield bank, but they were damaged by this activity.

And if we were ever able to catch the thief, are there sufficient criminal penalties to act as a deterrent? Does anyone know that?

Mr. SCHNEIER. So, it depends. Our laws are very, very nation-specific, and the internet is very international. So a lot of cyber crime comes out of Southeast Asia and Sub-Saharan Africa and Eastern Europe and places where we just do not have efficient enforcement and there is really jurisdictional arbitrage going on by cyber criminals.

And so, you know, enforcement works, but it really has limitations here. And that is why we really want to do what we can on the front end, because catching the bad guys, it is not going to work if it is a, you know, criminal organization in a country we just have no jurisdiction over.

Mr. BURGESS. But assuming we do stumble upon a bad guy, the proverbial guy in the basement who is doing bad things and hacking into things where they shouldn't, do we ever punish people like that?

Mr. SCHNEIER. Yes, all the time.

Mr. BURGESS. And what is the range—do you know what the range of punishments are?

Mr. SCHNEIER. I have no idea, but I am sure it is not pretty.

Mr. BURGESS. Do you feel it is a sufficient deterrent?

Mr. SCHNEIER. You know, that is probably a more complicated question I don't know enough to answer.

Mr. BURGESS. Yes. And I don't know that any of us do. But I do worry that—again, Equifax is a poor example, but sometimes it does seem like we victimize the victim in some of the things that

we do in punishing people who were the recipients of the breach, not the perpetrator of the breach.

Mr. Creighton, let me ask you—and I think, Mr. Schneier, you brought this up also. There is a great commercial out, where someone who—they get in a cab, and they have left—"Oh, my gosh, I left my debit card at the restaurant," and she doesn't think it is a big deal. Her companion has a near panic attack and meltdown. "Oh, my gosh, this is terrible. You left your card." And it turns out the person who left the card went on her phone and froze the debit card.

That seems like a very good approach if you knew that someone was accessing—so I guess let me ask you, Mr. Creighton, as a data broker, is there any way to notify people that their data is being accessed? Is there a system or could there be a system in place where—is there an app for that?

Mr. CREIGHTON. First of all, we represent the credit bureaus, not the data brokers.

Mr. BURGESS. OK. I beg your pardon.

Mr. CREIGHTON. But, yes, and those are coming online now and were coming on line in advance of the breach. TransUnion has their lock system up right now. It is free for everybody. It is at base, just like Mr. Schneier is discussing, where you can turn it on and turn it off.

Equifax has announced in this room that they will be offering a similar product that they are engineering now at the end of January. And Experian's is coming on line as well.

The point is to give the consumers that ability to easily go back and forth to lock their credit. It is different legally from a freeze, but it is meant to achieve the same goal without all of the cumbersome regulatory burdens that exist from the State governments.

Mr. BURGESS. Mr. Schneier?

Mr. SCHNEIER. I don't know anything about those. I like hearing that. I mean, the devil is in the details, so we would have to see the details, but that all sounds good.

I mean, that is really what we want. You want the user to get control. And I know when someone accesses my credit because I want them to; I am applying for something. Those feel like good things. And if they are simple to use, that feels like a really big step. It is not going to protect my data, but it is going to make it harder to monetize.

Mr. BURGESS. Which would be a good thing.

Thanks, Mr. Chairman. I will yield back.

Mr. LATTA. Thank you very much.

The gentleman yields back, and the Chair recognizes the gentlelady from California for 5 minutes.

Ms. MATSUI. Thank you, Mr. Chairman.

And thank you for the witnesses here today.

I find that every time we come to the hearings like this, I feel like the problem gets bigger and bigger, because the solutions are very disparate, and it is, kind of, very confusing, and there is not the simple solution that all of us want because we are all really very busy.

This commercial practice of collecting, aggregating, using, and selling consumer information has become functionally ubiquitous.

Companies and data brokers maintain databases full of sensitive and personal consumer information. These are natural targets for cyber thieves. But it is possible that an attacker can compromise one device using a known vulnerability and move readily within an information system to gain access to personal information.

Mr. Schneier, regardless of the method of attack, how would consumers benefit from comprehensive Federal standards that establish reasonable information security practices?

Mr. SCHNEIER. I mean, again, I think want to say the devil is in the details, right? You know, I want someone like the FTC to have some broad authority to figure it out. I mean, I don't think we can sit here and say, you know, here is what we should do.

There was a point made in that corner of the room that legislating the details will always lag technology. And I really think you have to start looking at what are the results we want. So I like the idea of, you know, a fine if data is breached. Let the companies figure out what to do, let the market work on the technical security solutions, but we want this particular outcome.

Ms. MATSUI. Right.

Mr. SCHNEIER. So those are the sort of mechanisms that I think will work best here.

Ms. MATSUI. OK. But I think the problem is also—the fact is we want to know, I think, that there is a Federal standard, whatever that is. Because right now everything is just all over the place.

Mr. SCHNEIER. Yes. I agree there has to be a Federal standard. And this is also what is going to be needed when we start dealing with international agreements.

Ms. MATSUI. Right.

Mr. SCHNEIER. What is the U.S. standard, and how can we assure the U.S. companies' European customers that we are not going to lose their data?

Ms. MATSUI. So you feel that this is going to be a necessary step anyway. Is that correct?

Mr. SCHNEIER. My guess is we are going to have to do this——

Ms. MATSUI. OK.

Mr. SCHNEIER [continuing]. That the world is moving that way. Europe is turning into the regulatory powerhouse——

Ms. MATSUI. Sure.

Mr. SCHNEIER [continuing]. And they are going to be leading us more and more.

Ms. MATSUI. Because we are reacting more than——

Mr. SCHNEIER. Yes. We are not going to like it, but I think we are going to be stuck with it, just because there is such a huge market.

Ms. MATSUI. OK.

Now, with all the consumer data that companies collect, we must keep pace with the evolving threat. Each year, we continue to see an increase in the variety, number, and damage caused by cyber attacks, yet relatively unsophisticated methods, such as phishing or emails with malware, remain some of the most common forms of attack. We have recently seen a decrease in zero-day vulnerabilities and an increase in simple exploits used to carry out attacks.

Mr. Schneier, how can both business and individuals better protect themselves against new applications of old exploits?

Mr. SCHNEIER. Well, so this is the definitive problem, that people are your weakest link. And we are certainly finding, you know, from nation-states on down, that the vector of going to the people—you know, Equifax was a vulnerability in the system. We talked about that. It is in many more cases that someone will get a person to do something. So tax fraud is a huge crime right now, and that basically involves convincing someone in HR to mail you a copy of everyone's W–2 and you file fake tax returns in all their names and you get the money. This is huge now, and it didn't exist 5 years ago.

Ms. MATSUI. Right.

Mr. SCHNEIER. And there are tech solutions that deal with this. And the problem is, as Mr. Norton talks about, is getting companies to use them, to make the purchase, to make things more inconvenient, for security.

Ms. MATSUI. How do we do that anyway?

Mr. SCHNEIER. That has to be incentives. The penalty for getting it wrong has to be more than the penalty for doing it right.

Ms. MATSUI. OK.

Mr. SCHNEIER. And that wasn't the case for Equifax.

Ms. MATSUI. OK.

I am also concerned about the question of who owns our user-generated data. You know, in 2014, agriculture technology providers and a coalition of major farm organizations came together to agree on data privacy and security principles to cover the massive data sets generated by innovation such as precision agriculture. These principles covered issues such as how data gathered from the farm is protected and shared. These principles also recognized that farmers owned the information generated by their farming operations, generally required farmers to be notified that their data is being collected, and required disclosure over how the data is used. But today's consumer has considerably less information over how, when, and what information is shared about them.

And I guess, Mr. Schneier, I am asking you this question, but somebody else can answer it too: Shouldn't consumers also have clarity over when and how their data is used?

Mr. SCHNEIER. Yes.

Mr. CREIGHTON. The Fair Credit Reporting Act goes into great detail about the seven permissible purposes that can be used for specifically credit reporting data. The other kinds of data that you are talking about, that is a different question. But in the credit reporting space, the Fair Credit Reporting Act is very firm about what exactly the information can be used for.

Ms. MATSUI. And when and how?

Mr. CREIGHTON. And when and how, yes. And by whom, yes.

Ms. MATSUI. All right.

I see my time has expired. Thank you very much.

Mr. LATTA. Thank you.

The gentlelady's time has expired, and the Chair now recognizes the gentleman from New Jersey for 5 minutes.

Mr. LANCE. Thank you, Mr. Chairman.

Good afternoon to the panel. Thank you for joining us today.

I am appalled by the scale and the impact of the Equifax breach. Equifax blatantly mishandled consumers' most personal informa-

tion. Constituents have called my office in New Jersey, concerned about their online security. And many were affected and their personally identifiable information compromised.

And, Mr. Norton, many organizations and individuals do not have up-to-date security or properly patched operating systems or software. What are some basic practical steps people can take immediately or in the short term to protect their computer systems?

Mr. NORTON. Absolutely. Thank you.

You know, something as simple as changing your password, you know, once a week or once a month and taking those logical steps; making sure that you have, you know, appropriate software security that is publicly available in the marketplace for your home computers; that you are aware of your devices and you have passwords on, you know, all of your devices; that you are constantly aware of, you know, information that you have that is out there.

I mean, cybersecurity really requires a lot of individual vigilance, which is a big change, I think, for a lot of consumers at home who are, you know, in the marketplace and they have their information online and they become very used to just processing things online, as we talked about in this hearing.

I think one of the challenges, though, is that we haven't actually put a value on loss of data, what does it mean to lose your individual person's piece of data, outside of just getting, you know, a piece of credit reporting for a year, you know, what is the other value of that. And I think that is another discussion or a large discussion that you are obviously having here, but I think it is an important one, and it goes to, you know, potential penalties or things that could motivate companies to then, you know, have larger enforcement and larger strategies within their businesses. So I think there is that, as well.

Mr. LANCE. Thank you.

Would anyone else on the panel like to comment?

Mr. SCHNEIER. The unfortunate thing is that most of our data is not under our control. So what can you do to protect your data at Equifax? Nothing. What could you have done to protect your data at the OPM? Nothing. What can you do to protect your data at Google? Kind of nothing. We are forced to trust these entities.

These companies have our data. Our pictures are stored on Flickr, and our email is on Gmail, and our computers really have very little right now. In some ways, that is a security bonus, because most of us aren't very good at securing our machines. But it does mean that these breaches become bigger and more catastrophic because we have too much there.

I mean, there are things we can do around the edges—good password management, have antivirus. I mean, I can rattle through the tips. But, by and large, the security of our data is not under our control.

Mr. LANCE. Thank you very much.

Ms. Fortney, are you aware of the Consumer Financial Protection Bureau's bringing any enforcement actions against a credit bureau?

Ms. FORTNEY. The Bureau does supervise the agencies. They have brought enforcement actions, not in the area of data security, but they have brought enforcement actions against the credit bu-

reaus. And I think they are also involved in the ongoing investigations that are the result of the Equifax breach.

Mr. LANCE. Thank you.

Mr. Creighton, what is the credit lock product that the major credit bureaus are proposing, and how are they different from credit freezes?

Mr. CREIGHTON. Thank you. That is an important question.

First of all, the bureaus are responding to consumer demand, as Mr. Schneier was saying, that they want more access to their information and how they can control it. And, right now, State law mandates, in most States, a freeze. Those freezes are different in every single State, and they are often PIN-based. And so what happens is that you put a freeze on your account, you get a PIN. If you are like me, you then lose that PIN. And when you go back——

Mr. LANCE. Or like me. Yes.

Mr. CREIGHTON. Right. And when you go back and you try to get a new iPhone, as has been reported this week, people don't realize that that is a credit transaction, they don't have their PIN, they can't turn it off, it takes 3 days, and they have missed the window to order the new iPhone.

Now, the lock product functionally works the same way. It is app-based. And it allows a consumer to turn it to red, "I don't want any new offers of credit," and when I do want an offer of credit, I flip it to green.

Mr. LANCE. I see.

Mr. CREIGHTON. But it doesn't contain the same legal strictures that happen as a result of State law.

Mr. LANCE. Well, thank you very much. This is very interesting, and I hope that we are able to pursue it further.

And, Mr. Chairman, I yield back 10 seconds.

Mr. LATTA. Thank you very much.

The gentleman yields back, and the Chair now recognizes the gentleman from Indiana for 5 minutes.

Mr. BUCSHON. Thank you, Mr. Chairman.

I want to make a couple of quick comments, and then I will have a few questions.

First of all, I think it is important, potentially, to understand that we authorize a lot of people to get our data unsuspectingly. And, I mean, for this card, for example, here—I don't want to hold—it is just a card that goes to a grocery store, right? That gives you your discount. All that data is collected. You have authorized it, when you signed up to the card, you have authorized it to be sold for any reason. Same thing is true on your emails. Same thing is true everywhere.

You know, I used a search engine yesterday. I have a piano I want to sell. Today, on my Instagram, an add for a piano came across my Instagram, OK?

I have used credit agencies because I have some rental property. Mostly, the people have to authorize you to get their information. So there are protections there where they have to authorize it.

The point I am making is that this is a really complicated problem. We are talking about a breach. That is not that complicated, because we had human error that didn't patch. That is pretty straightforward. But we do have a larger problem with data, we

have a larger problem with internet, that all of us are working to figure out how do we best protect the consumer.

I do have concerns about these long legal-department-generated authorizations that are attached to all of these things. And I do think we may have to look at that area and make consumers more aware of what they are actually authorizing.

I mean, what do you do? You go and start an email account, and you get to the end, and it says, you know, unless you agree to these things, you can't start it, I mean, you can't do it. And most of us just click—I mean, does anyone here just click "agree" without reading it? Right. I mean, we all do. But that is actually a legal document that is very long that has specific legal ramifications that seem simple but aren't.

I mean, you know, you do a search engine on a piano, and the next day on your Instagram account you have piano ads. I mean, that is kind of spooky. Everyone is concerned about the NSA. I am more concerned—I am concerned about that, but this type of thing.

So the question I have, you know, Mr. Creighton, first of all, it has been about 3 months since the Equifax breach, yet still thousands of Americans are unaware if their data has been stolen. Do you think that—you know, 48 States have conflicting State notification laws that have played in this issue. And do you believe that a uniform Federal law on notification might address the difficulties with Americans receiving notification?

Mr. CREIGHTON. Consumers would benefit from a national data breach notification.

Mr. BUCSHON. OK. So the answer is, yes, they would?

Mr. CREIGHTON. Yes, sir.

Mr. BUCSHON. The other thing is, when we had the Equifax CEO here, honestly, in fairness to him, I thought he was a genuine witness. You know, there were issues, but I think his testimony was genuine. But there were flaws in their system of reporting within their company; I understand that.

But, you know, one thing that was brought up is—I represent a rural area of the United States. And he was talking about getting online and going to their website and seeing all the things that you can do to protect yourself and all that. I think we all have to recognize the fact that even in the United States—I mean, I think the penetrance of internet access in my district may be about 65 percent of the people, believe it or not, maybe 70 percent. That leaves 30 percent, 35 percent of the people out there that they just can't pull up a website and see.

I mean, how can we address notification or this type of thing or best practices in an age where—I think all of us mentioned, "Well, their websites show us this," right? But 30, 35 percent of the people I represent may not have internet access.

Mr. CREIGHTON. Congressman, it is a big problem. And reaching rural consumers is one of the big challenges. That is why, when we talk about the lock product, for example, it doesn't mean we aren't still obligated to offer the freeze product, because you have to maintain call centers and other things so that people have access.

But the credit reporting system serves probably your consumers, your constituents, better than anybody else. A rural consumer generally has one physical bank near them, right? But in today's

world, you, as a consumer, even a rural consumer, can access the entire world of credit available to you. If you are getting a mortgage, you don't——

Mr. BUCSHON. Right. I get all that. What I was trying to get at is that I think we have to recognize that not everyone out there that has had their data breached because they have gone to their local bank to get a loan can be notified that they have been compromised by telling them to go to a website.

I mean, I don't know how else we address that. I addressed this same question with the CEO of Equifax. And we are advancing, I think, a lot in consumer access to information. But one area, I just think people have to recognize, across rural America, necessarily, people don't have access to that information. We need to do a better job.

I yield back.

Mr. LATTA. Thank you.

The gentleman's time has expired, and the Chair now recognizes the gentleman from Oklahoma for 5 minutes.

Mr. MULLIN. Thank you, Mr. Chairman.

And thank you to the witnesses for being here.

Mr. Norton, I kind of want to start with you. Just in your opinion, does the current Federal regulatory structure, does it have enough safety safeguards in it for the consumer?

Mr. NORTON. You know, I think it is a matter of corporate responsibility and whether or not they are, you know, making the appropriate investments. And, clearly, they are not, from the top down. I think that is why we are seeing these things.

Mr. MULLIN. And that leads me to my next point. As a manufacturer, if you manufacture a product, and even if the product is misused—like, inside my district, we had a gas can company that essentially went out of business because of all the litigations about, you know, the problems with the gas can. And what was happening was people were literally pouring the gas right out of the gas can on a fire and they were catching fire. Obviously not the smartest thing to do, right? But they were still open for lawsuits. They still had a responsibility, for whatever reason, to the consumer, even though the product was obviously being misused, outside its manufacture and design.

We had these websites—and, Mr. Schneier, you brought this up—that you are vulnerable. I don't care what you do, you are vulnerable. Where does the responsibility lie? Is it just on the consumer? Either one of you guys can answer this. Is it just on the consumer?

Mr. NORTON. No. Absolutely, I think that it is—consumers certainly can help drive the market and change the market, and hearings like this will help, I think, drive corporations to accept further responsibility. I think it goes back, again, to not putting a value on data, as an individual. Companies have put a value on it, but we haven't put a value on it, in terms of loss of data, as the individual.

Mr. MULLIN. But, as Mr. Schneier said, we can safeguard ourselves—there is a huge difference between a manufacturing product being misused by the person holding the product versus a consumer that has no idea what has happened to their data. They are

letting it be sold, it is going out there without our intention. So we are not even not using it within the manufacturer's instructions; it is the manufacturer—I am breaking it down to layman's terms. It is the holding company that has our information that isn't safeguarding it to begin with. And we are the ones paying for it. Where do the responsibilities lie?

Mr. SCHNEIER. I think your analogy is good, that we definitely have consumer misuse, but you actually have fundamentally unsafe products.

Mr. MULLIN. Right.

Mr. SCHNEIER. And, in those cases, you really need to hold the designers, the manufacturers, the data holders, the app makers, the system makers responsible to some degree, that we cannot have a system where you have to be an expert in order to survive in the 21st century.

I mean, I don't want to be an expert in gas cans to be able to use that product. And maybe I am going to do something stupid, but I would like it if the system prevents me, as much as possible, from doing something stupid. And——

Ms. FORTNEY. I would like to——

Mr. SCHNEIER [continuing]. That is sort of a way of thinking about regulation.

Mr. MULLIN. Ms. Fortney?

Ms. FORTNEY. I would like to address that.

I think, first of all, there are consequences for companies that do not secure consumers' data, and there are penalties that can attach. There is an enforcement regime by the Federal Trade Commission, the Consumer Financial Protection Bureau.

In addition, I think the question is, what should consumers do when they have the information that their data is being used and that it could be breached? Because I think, no matter what we do, no matter what security procedures are there, given the many, many attempts from all over the world to access data that is being held in any type of large database in the United States, there is the risk of a breach. And I do think that what consumers need to do is really know more about what they can do to protect themselves.

We are talking about notice here, and one of the notices that we haven't really focused on is a notice required under the Gramm-Leach-Bliley Act——

Mr. MULLIN. But we are talking—we are talking about notices. That is not good enough. There is a difference. They enter in that business taking a risk, the same thing as a manufacturer enters a business in taking a risk too.

Ms. FORTNEY. Right.

Mr. MULLIN. We don't see insurance policies paying off to those consumers that were breached by Equifax. Whereas, with a manufacturer, if something happens, you see insurance companies. That is why they have insurance. They are stepping up and taking responsibility for it. We are not seeing that in the digital world. We are seeing it as, "Well, that is the risk of being online." And I take that risk seriously.

But it seems like there is a disconnect. "Well, we know it is going to be breached. There are cyber issues going on out there." But that

is the business that they are in.A consumer ought to feel safe about doing business with that person, not always constantly being concerned.

All of us up here have had our credit card stolen. I am currently, right now, on my fifth credit card with this one company this year alone because it has been——

Mr. SCHNEIER. What is the number?

Mr. MULLIN. Evidently it is out there someplace.

But we are just looking at how—I am not looking to put more regulations or more burdens on the companies, but there has to be a sense of responsibilities for the consumer to feel safe, because just notifications is being reactive, not proactive.

Ms. FORTNEY. Yes, but I began my remarks by saying there are penalties for breaches. And then the next question is, what can consumers do once there has been a breach? And I think there are remedies available.

Mr. MULLIN. I am out of time. I apologize, Mr. Schneier. I would love to hear your response on it, but I am out of time on it.

Mr. Chairman, I yield back.

Mr. LATTA. Well, thank—I am sorry?

Ms. SCHAKOWSKY. Can I ask another question?

Mr. LATTA. The gentlelady is recognized for one other question.

Ms. SCHAKOWSKY. Oh—sorry. Sorry.

Mr. LATTA. OK. Just wanted to make sure. I thought you may have coordinated there.

The Chair now recognizes for 5 minutes the gentleman from Texas.

Mr. GREEN. Thank you, Mr. Chairman. I want to thank the chairman and ranking member for holding this hearing.

I appreciate the time of our witnesses.

While the recent data breach at Equifax is bad enough on its own right, it also has shone a light on several larger problems. The first is the lack of knowledge or control over who collects information on us and what information they collect and what they do with it.

In 2014, the FTC issued a report recommending Congress enact legislation to make the data-broker industry more transparent following the Equifax breach. It is a good time to take a closer look at these issues.

Mr. Schneier, in your testimony, you state that the data brokers collect information on everything that we do on the internet. Can you elaborate on the scope of the information, such as what kinds of data are collected and how many of our transactions on- and offline are recorded or collected by data brokers?

Mr. SCHNEIER. So that is hard, because it is collected in secret, and we actually don't know. We see shadows of it. We see shadows of it in the lists that they sell.

And this is data brokers writ large. This is not credit bureaus specifically.

So you will see them selling lists of, you know, seniors who have debt problems; or, you know, people who have particular medical conditions; or interest groups of, sort of, any unimaginable distinctions. And you often can go and look at the different types of lists that are sold.

But the industry is really so opaque that we don't know. We just know that it is all being—whatever can be collected is being collected. We really don't know how it is being used. You know, we are hearing a lot about some big-data analytics were used in the last election. We don't know the details of that.

It is a very opaque industry. It makes your question much harder to answer than it should be.

Mr. GREEN. OK.

In the FTC's 2014 report, one of the FTC's recommendations was the creation of a website to let consumers see what information data brokers have on them and to opt out of having it shared in the future.

Mr. Schneier, can you talk a little bit about this particular suggestion and what the obstacles would be to create such a website?

Mr. SCHNEIER. The obstacles would be that the companies don't want to do that and that, if they did it, it would be kind of horrific.

This is a story from Europe, because Europe has laws that require some kind of disclosure. And Max Schrems, who is a law student, sued—successfully in a European court—Facebook to get all the data Facebook had on him. And he got a stack of paper 1,000 sheets high of all the data Facebook had on him. And Facebook has that data times everybody who is on Facebook.

Mr. GREEN. OK.

You mentioned that data brokers operating in Europe can and do follow the EU's more stringent privacy laws. Can you compare for us the difference between the scope of personal data collected in the European Union versus the United States, particularly regarding our online activities?

Mr. SCHNEIER. So I am not an expert, and I would hesitate to do that. That is an important question to ask, and there are people who are doing that research.

Europe has rules about what can be collected and under what circumstances, how it can be stored, how it can be used, and how it must be deleted. You might have heard about the right to be forgotten, which is a contentious European law.

European law is very complicated here, and it is still under a lot of change. So that is an important question. I really want you to find someone who is an expert in that to talk to that.

Mr. GREEN. Well, it seems just common sense that data knows no boundaries. They don't know the borders of the United States or Europe. It seems like our country should partner with the EU and other countries to see if we can coordinate our regulations on this.

Because I think, if you heard the questions earlier and listened to them, our data should be our data, and we should be able to have control over who looks at it, instead of just deciding that maybe "I think I need a new car" and send me something. But I think that is what we need to do.

Mr. Chairman, thank you all for holding the hearing, and it brings up a lot of issues we need to deal with. Thank you.

Mr. HARPER [presiding]. The gentleman yields back.

The Chair will now recognize Mr. Bilirakis from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you. Thank you, Mr. Chairman. I appreciate it.

I thank the panel for their testimony today.

Mr. Creighton, some consumers have suggested to me to minimize the identifiable data collected, like using partial Social Security numbers or partial driver's license identification.

Is this possible for CRAs to do? And would it help better protect consumers from bad actors not authorized to use such data?

Mr. CREIGHTON. Social Security numbers are used as identifiers, and they are important identifiers. They are not used, necessarily, by financial institutions to authenticate a consumer, but they are used to identify them.

And that is important because you have a lot of people in this country, a shocking number, really, when you look at it, who have similar names, similar dates of birth, similar Social Security numbers. Having the full 10-digit Social Security number is going to be helpful for making sure that we have the right person that we are able to match.

And we have an obligation under the Fair Credit Reporting Act to make sure that we are matching the correct data with the correct person.

Mr. BILIRAKIS. How about using the driver's license identification? Wouldn't that suffice?

Mr. CREIGHTON. Well, not everyone has a driver's license, first of all. And, you know, whether we like it or not, the Social Security number has, in effect, in the United States, become a universal identifier. And it is the one piece of information that crosses over many different databases, particularly in the Government.

Mr. BILIRAKIS. And you think you have to use all nine numbers as opposed to——

Mr. CREIGHTON. Yes. I mean, now, there are a number of statutes around the country where the minimization of the Social Security number has led to issues. For example, on credit reports today, it is much harder to know what all the liens and judgments you may have against you are, because in certain courts you no longer have full Social Security numbers and so we can't do the full match. And since we can't do the full match, we have just taken off a lot of that data.

That degrades the entire credit reporting system. It is a little bit less complete because of that. And that is problematic, because if you are a lender, in order to make a safe and sound lending decision, you should know the full set of obligations that a consumer has.

Mr. BILIRAKIS. Thank you.

Mr. Norton, are there one or two recommendations you can make for the small- to medium-size companies with limited resources that are most effective in limiting vulnerabilities to criminal hacking?

Mr. NORTON. Yes, absolutely. I think that small businesses, obviously, are the most at risk, number one, because they do have those limited resources. Typically, a small business could be, you know, just a handful of people, and, you know, what kind of investment do they need to make internally?

And I think just starting that conversation amongst the small businesses is an important step and just saying, OK, look, we have X number of computers, X number of people that can access our database. So I think, just internally, alone, starting there and saying, OK, do we have, you know, the appropriate passwords, you know, do we need some type of encryption on our network that can be publicly available and brought in the marketplace, you know, do we have a point person within the business, and even if the business has three people, somebody that is responsible for that, and just kind of having those access controls I think is a good starting place for small businesses.

And then the larger businesses, I would say it is a very similar model, in terms of maybe you are getting to 50 or 100 but, again, starting to carve out, you know, as they look at their outyears and starting to develop a strategy of, OK, you know, in this calendar year, whenever their fiscal year starts, this is how much money we are going to start to invest in this particular area, which is just as critical as keeping the lights on or paying the gas bill or paying employees' salaries. It has to become part of the day-to-day culture. And I think that is an important conversation they need to have just to start to secure themselves.

Mr. BILIRAKIS. Thank you very much.

My third question, again, for Mr. Norton or Ms. Fortney. Is there a legitimate worry about criminals using consumers' data to establish a Social Security Administration online account in their name and claiming their benefits? Where or how does a victim go about to protect oneself in that scenario?

You both can answer the question. I do have some time.

Ms. FORTNEY. I assume that there are protections there, but this is not an area where I have worked. I focus primarily on credit reporting, the credit industry, and other aspects of data security. I would like for Mr. Norton to address it.

Mr. BILIRAKIS. Yes, please.

Mr. NORTON. Of course, there are some, you know, steps you can take in terms of, if you believe you have been a victim of, you know, some sort of fraud, contacting the Social Security Administration and letting them know. And I believe there are some things you can fill out to let them know.

I think it is also not the easiest process in the world. I think that is one of the challenges for the individual consumer, is the fact that, what does somebody do? You know, you can't really necessarily go down to a police station and fill out a police report just the same way as if somebody robbed your home and took your TV and a couple other things. This is a very different problem, and I think that that is part of the challenge here.

And it is just like we were discussing earlier. Not everybody can go online and fill out paperwork or, you know, have the ability to even call. And so doing things in a more efficient way and finding ways for, you know, kind of, one point of entry, not 19 Government agencies for the individual consumer and individual small business, I think would be another important step for this subcommittee to help for the consumers.

Mr. BILIRAKIS. OK.

Thank you very much, Mr. Chairman. I will yield back.

Mr. HARPER. The gentleman yields back.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Costello, for 5 minutes.

Mr. COSTELLO. Thank you.

I would like to ask my questions and then offer some observations so that each of you can think it through.

Ms. Fortney, in your written testimony, you mentioned the updates that were made to the FCRA in 2003, which included new measures to protect consumers from identity theft and other unauthorized use of the data they have on file with the CRAs.

Do you believe extended fraud alerts are a sufficient recourse option for consumers who wish to remain credit-active but want to opt in?

Second, are you aware of any backlogs or delays in the process related to extended fraud alerts? And, if so, do you have any suggestions on how to streamline consumers' access to these and other protections available?

And then the next question to all witnesses: What would be the most effective means of reducing the administrative burden so victims of data breaches can protect themselves from credit fraud without facing impediments to obtaining credit if and when they need it?

And then, finally, Mr. Schneier, you state, "Congress should not create a new national identifier to replace Social Security numbers. That would make the system of identification even more brittle." I would like you to elaborate on that.

Many of my constituents who were impacted by the Equifax data breach have shared with me numerous frustrations they continue to face both in dealing with the immediate aftermath of the breach and in trying to find the best path forward to prevent the fraudulent use of the information that was compromised. What I find frustrating is that so much of this burden falls on the consumers.

In the case of the Equifax breach, nearly 50 percent of the U.S. population can be considered a victim. With half our Nation directly impacted by this breach and millions more affected by other recent data breaches, it is astounding to me and my constituents that so much of the burden remains on consumers and that they have to deal with it themselves, first by determining whether they were impacted, then by figuring out what makes the most sense in terms of monitoring or freezing their credit and dealing with all the administrative hurdles and potential barriers to credit that go along with it.

I would imagine many people might not know where to start or become so frustrated in trying to stay ahead of identity theft that they give up trying and instead resort to dealing with fraud if and when it occurs instead of using the resources that may be available to protect them against further harm.

And, with that, the questions that I asked, if all of you would answer.

Ms. FORTNEY. OK. Thank you.

First of all, fraud alerts are a useful tool for someone who thinks they might be a victim of identity theft or might become a victim of identity theft. In order to get a fraud alert, the consumer goes on the website of one of the three major credit bureaus, puts in the

necessary information, and does get the alert. There is not an inquiry into the request for an identity theft report or anything of that kind. So I think it is a relatively streamlined process.

I think the other thing to keep in mind is that, when we are looking here at credit reporting data—because Equifax is a credit bureau—we need to focus on the fact that there are a lot of provisions in the Fair Credit Reporting Act that were enacted in 2003 to prevent identity theft. There are certain rules in terms of address discrepancies. There are rules that require furnishers to identify the consumers before they provide the information.

So I think there are a lot of protections in the Fair Credit Reporting Act because we are focusing, in the case of Equifax, primarily on data that involved the credit bureau.

Mr. SCHNEIER. I am going to quickly address your Social Security number question.

Mr. Creighton is right that a Social Security number is actually a pretty good identifier. Name and birth date is terrible, too many duplicates. We have learned that from attempts to purge voter rolls. And a Social Security number is something everybody has.

Where it fails as an authenticator, where it fails is that knowledge of it proves that you are you. It is a public number and shouldn't be treated as a secret or any kind of authenticator. So I don't think we need to replace it. I think it works just fine as long as we recognize its limitations.

We are much better off, instead of one large authentication system, where a failure in it is a catastrophic failure, to have multiple context-specific authentication systems. Just like you have a dozen cards in your wallet, they do different things, there is no real reason why it can't just be one card except——

Mr. COSTELLO. Do you find that implementable? Do you find that implementable for——

Mr. SCHNEIER. Yes, I think we can. I mean, you will see it—you see it on your phone. You have lots of different authenticators. Again, there are many different sites. They all work through your phone. Industry does figure this out. It is complicated, but, yes, I do think it is doable.

Mr. CREIGHTON. Congressman, your second question was can we be more helpful to consumers who want to lock their credit or freeze their credit or something like that. And these new products that are coming on the market now—TransUnion already has it; the other two bureaus have them coming out now—that allow people, on an app-based system, to lock and unlock their credit.

Mr. COSTELLO. Right.

Mr. CREIGHTON. The other thing is more and more credit card companies are including your credit score on their statements. And that is a good way for you to just check and make sure that there are no changes from month to month that you weren't expecting.

Mr. COSTELLO. Thank you.

Mr. HARPER. The gentleman yields back.

The Chair now recognizes the gentlelady from California, Mrs. Walters, for 5 minutes.

Mrs. WALTERS. Thank you, Mr. Chairman.

Last month, this subcommittee began an investigation into the Equifax breach that resulted in the theft of 145 million Americans'

personal and financial information. Equifax failed in their legal obligation to protect consumers.

Today, we continue our work to ensure the consumers' information is secure and that companies are taking adequate security measures to protect their sensitive data. It is vital that we confront these security challenges so that our digital e-commerce continues to develop and helps fuel the American economy.

Ms. Fortney, we have discussed the regulatory framework. Do you believe the regulatory framework for CRAs is sufficient to protect U.S. consumers from data breaches and satisfy consumers' privacy concerns?

Ms. FORTNEY. Yes, I do. And I can say that having worked with the Fair Credit Reporting Act for more than 40 years. I have seen this act amended by Congress several times as new concerns arise. And, as we mentioned, in 2003, because people were becoming increasingly concerned about identity theft, new provisions were put in the act.

The act imposes really strict requirements on consumer reporting agencies with respect to the accuracy of the information, the provision of credit reports to people who only have very definite permissible purposes.

The act provides for notice to consumers when the information has been used on them in a way that is adverse to their interests.

I could go on and on. My written statement has many, many protections here.

I think the question really is, is there anything in the Fair Credit Reporting Act or other law that resulted in the Equifax breach? In other words, was there any deficiency in any of these laws? And I think we don't know the answer to that because we don't know exactly what the circumstances were that led to the Equifax breach.

What we do know is that, by and large, we have one of the, if not the most robust systems of credit reporting and consumer reporting generally in the world. We have one of the strongest economies in the world. You start taking away some of the benefits, if you start over-regulating this industry and you start allowing people to remove information from the system, the system is not going to work as well.

And I think all you have to do is compare our system to that of other countries, including developed countries, that don't have credit reporting systems that are as comprehensive, and I think you will see there are a lot more benefits to consumers.

Mrs. WALTERS. This question is for you, again, the next one. What level of responsibility should lenders, banks, credit unions, insurers, et cetera, demand from CRAs when they are the purchasers of a credit reporting product?

Ms. FORTNEY. What measures should they demand?

Mrs. WALTERS. What level of responsibility should lenders demand from CRAs?

Ms. FORTNEY. Again, the level of responsibility is in the Fair Credit Reporting Act, has been for many years, and that is that the consumer reporting agency that is providing the credit report must identify the recipient of that report, must be able to authenticate that this is somebody who has a permissible purpose under the

statute to receive the report. And I think that is something that has been at the heart of the Fair Credit Reporting Act from the beginning.

Mrs. WALTERS. OK.

Mr. Creighton, is there any type of financial or personal data that is illegal or impermissible for CRAs or data furnishers to collect and possess?

Mr. CREIGHTON. Oh, there are multiple. I mean, you can really only collect certain kinds of data at credit reporting bureaus, not referring to the larger data brokers. It is basically just, you know, your identifying information; whether there are any public liens or judgments against you, like a bankruptcy; do you have credit, from whom, how much; your balance; and do you pay on time. And that is all regulated by the Fair Credit Reporting Act.

After that, you are outside of the Fair Credit Reporting Act, and so you are in a different regulatory scheme.

But the Fair Credit Reporting Act, as I said in my testimony, is a very important and very strong consumer protection statute that has criminal penalties, it has transparency requirements. It is probably the model on which you are all going to work from if you do go down the path for other data broker information.

Mrs. WALTERS. OK. Thank you.

And I yield back the balance of my time.

Mr. HARPER. The gentlelady yields back.

The Chair will now recognize Ranking Member Schakowsky for a followup question.

Ms. SCHAKOWSKY. Thank you.

Mr. Schneier, you were just shaking your head on the idea that I think that Mr. Creighton was saying, that it is very strictly regulated, what kind of information that they could have. I just wondered if you wanted to add something else.

Mr. SCHNEIER. So, I mean, I am thinking of the data brokers writ large. I mean, yes, the credit bureaus are regulated, what they can collect, but the data brokers can collect everything. I mean, Google knows what kind of porn we all like, because that is how we search it, and they can collect that.

So, as you move out from the very narrow place we have regulated, all bets are off. And I think we really need to look at how this bigger industry is moving and not just credit bureaus.

Ms. SCHAKOWSKY. OK.

So I understand, I think, what your association does. But Equifax has a business outside of being a credit reporting agency. So what I am trying to understand, does your trade association then deal with the rest of that? And are they not also a data broker?

Mr. CREIGHTON. Yes, they are. Not all of my members are data brokers. What we do specifically at CDIA is the—we are, essentially, the Fair Credit Reporting Act association. So we represent the credit bureaus inside the companies. That is really, very narrowly, what we do, is the Fair Credit Reporting Act-governed databases that they have, the companies that do it, the credit bureaus.

Ms. SCHAKOWSKY. The databases. But those same companies—well, first of all, even under their credit reporting data function, they can sell to advertisers who offer credit, right?

Mr. CREIGHTON. Some offers of credit, yes. Prescreened, firm offers of credit. That is correct.

Ms. SCHAKOWSKY. OK. But I don't want those cards.

Mr. CREIGHTON. You can opt out, though.

Ms. SCHAKOWSKY. This is—excuse me?

Mr. CREIGHTON. You can opt out of prescreened offers. That is an option that you have as a consumer, to opt out of prescreened offers.

Ms. SCHAKOWSKY. Who knows that?

Mr. SCHNEIER. Yes, good luck figuring out how.

Ms. SCHAKOWSKY. I am sorry?

Mr. SCHNEIER. Good luck figuring out how.

Ms. SCHAKOWSKY. Yes. I mean——

Ms. FORTNEY. Every prescreened solicitation contains a notice that the Federal Trade Commission has determined must be placed there—it must be clear and conspicuous—telling consumers that receive these prescreened offers that they have received the offer because of prescreening and telling them how to opt out.

Ms. SCHAKOWSKY. You know, I will tell you—and maybe it is like those security, you know, 12-, 10-point, 8-point notices that we all get and that we all press "agree." I mean, really—and I think that is just—and I heard your whole list of things that we can do to protect ourselves. And I am sure you are in the 1 percent that actually can do that. This is really a lot of work for people who even have the ability on the computer.

But I wanted to ask you something else. So, to the extent, though, that Equifax is a data broker, you have no relationship to them?

Mr. CREIGHTON. No. We are specifically representing them on the credit bureau part of the——

Ms. SCHAKOWSKY. OK. I want to quote what you said at the very beginning. You said, "The scale of the criminal act at Equifax was unprecedented." I checked back with the record.

Mr. CREIGHTON. "Breathtaking," I think——

Ms. SCHAKOWSKY. So what do you mean? What is the criminal act?

Mr. CREIGHTON. Well, information on 145 million people was released. It was not information from the credit bureau. It was not the credit file information. That database is about 220 million people. It was not that file. It was a file that they had that included other kinds of information that they collected in other ways.

Ms. SCHAKOWSKY. So what law did they break?

Mr. CREIGHTON. Well, under the Federal Trade Commission Act, they probably committed a—I mean, we should let the investigation play itself out so that we know. But I would suggest that they probably have UDAP problems. And then they also have—I mean, I would defer to counsel who might know better——

Ms. SCHAKOWSKY. Well, I want to, you know, home in on——

Mr. CREIGHTON. Look, I mean, they are going to have——

Ms. SCHAKOWSKY. You said very unequivocally, "The scale of the criminal act at Equifax was unprecedented"—"criminal act at Equifax."

Mr. CREIGHTON. So I am talking about the——

Ms. SCHAKOWSKY. I mean, I tend to feel that that is true. But, as an expert on this, I want to know——

Mr. CREIGHTON. Right. No, I was referring specifically to the hackers being criminals. Right? I mean, let's remember that whoever broke into this system did not do it legally. They were criminals who broke into Equifax. And we don't know what their motives were, but they were criminals who did this. It was a criminal hack, it was a criminal attack on an American company, is the point I was trying to make.

Ms. SCHAKOWSKY. OK.

Thank you. I yield back.

Mr. HARPER. Seeing that there are no further witnesses wishing to ask questions, I want to thank each and every one of you for taking the time to be here today.

Before we conclude, I would like to include the following documents to be submitted for the record, by unanimous consent: one, the written statement of Jeff Greene, Senior Director of Global Government Affairs and Policy, Symantec; and a letter from the Electronic Frontier Foundation.

[The information appears at the conclusion of the hearing.]

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

Without objection, this subcommittee is adjourned.

[Whereupon, at 12:44 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Prepared Testimony and
Statement for the Record of

Jeff Greene
Senior Director, Global Government Affairs & Policy
Symantec Corporation

Hearing on

Securing Consumers' Credit Data in the Age of Digital Commerce

Before the

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

November 1, 2017

Chairman Latta, Ranking Member Schakowsky, my name is Jeff Greene and I am the Senior Director, Global Government Affairs and Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. I also serve as a member of the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board (ISPAB), and last year I supported the President's Commission on Enhancing National Cybersecurity. Prior to joining Symantec, I served as Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues.

Symantec Corporation is the world's leading cybersecurity company, and has the largest civilian threat collection network in the world. Our Global Intelligence Network™ tracks over 700,000 global adversaries and is comprised of more than 98 million attack sensors, which record thousands of events every second. We maintain nine Security Response Centers and six Security Operations Centers around the globe, and all of these resources combined give our analysts a unique view of the entire cyber threat landscape. Symantec also provides identity theft protection to over 5 million Americans through LifeLock, a leading provider of identity theft protection and comprehensive remediation services for consumers.

Cybersecurity is the foundation of the age of digital commerce, and we are therefore pleased to see the Committee's continued focus on this subject, and appreciate the opportunity to provide our insights. The threat to consumers, and in particular their personal and credit data, is best understood in the context of the larger cyber threat landscape. In my testimony I will briefly discuss the broader cyber threat environment and then discuss securing enterprises and consumers against an evolving threat.

I. The Current and Emerging Cyber Threat Landscape - Overview

Cyber attacks reached new levels in the past year, which was marked by multi-million dollar virtual bank heists, explosive growth of ransomware, attempts to disrupt the US electoral process by state-sponsored groups, a record number of identities exposed in data breaches, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices. Yet while the attacks caused unprecedented levels of disruption and financial loss, perhaps the most striking change over the past year is that in many cases the attackers used very simple tools and tactics. During 2016, valuable Zero-day vulnerabilities and sophisticated malware was used more sparingly than in recent years. Instead, attackers increasingly attempted to hide in plain sight. They relied on straightforward approaches, such as spear-phishing emails and "living off the land" by using tools on hand, such as legitimate network administration software and operating system features. Yet despite this trend away from sophisticated attacks, the results were extraordinary, including:

- Over ***1.1 billion*** identities exposed in 2016;
- ***Power outages*** in the Ukraine;
- Over ***$800 million*** stolen through Business E-mail Compromise (BEC) scams over just a ***six month period***;
- ***$81 million*** stolen in one bank heist alone;
- A ***tripling*** of the average ransomware demand;
- Average time-to-attack for a newly connected Internet of Thing device down to ***two minutes;***
- And of course, the theft of over **145 million identities** from Equifax earlier this year.

Cyber attacks involving sabotage have traditionally been rare, but during 2016 we saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in the attacks on the Ukraine in January and again in December, resulting in power outages. Additionally, the disk-wiping Trojan Shamoon reappeared after a four-year absence and was used against multiple

organizations in Saudi Arabia. Previously, Shamoon was used in highly destructive attacks against Saudi and other Middle Eastern energy companies, and press reports linked it to Iran.

On the financial side, cyber criminals have broadened their targets. While in the past they mainly targeted individual bank customers, raiding accounts or stealing credit cards, over the past year we saw a new breed of attacker with bigger ambitions. We now see groups targeting the banks themselves, sometimes attempting to steal tens of millions of dollars in a single attack. For instance, the Lazarus group stole $81 million from Bangladesh's central bank by exploiting weaknesses in the bank's security to infiltrate its network and steal its Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials. And while the attackers did make off with $81 million, it could have been much worse as they attempted numerous other transfers that were detected because a spelling error in a recipient's name raised suspicions that led to the transactions being suspended.

Criminals also target major corporations, and have found success stealing huge sums of money through relatively unsophisticated means. For instance, business email compromise (BEC) scams – which rely on little more than carefully composed spear-phishing emails – continue to cause major losses. Also known as CEO fraud or "whaling," BEC scams are a form of low-tech financial fraud where spoofed emails are sent to an organization's financial staff by scammers pretending to be the CEO or senior management. The scammers then request a large money transfer. These scams require little technical expertise but can reap huge financial rewards for the criminals – and significant losses for the companies involved. Earlier this year the FBI issued an alert noting that "[b]etween January 2015 and December 2016, there was a 2,370% increase in identified exposed losses" from BEC scams. The FBI estimated that over $5 billion was lost to BEC scams between October, 2013 and December, 2016.[1] In 2017, approximately 8,000 businesses have been targeted by BEC scams each month, and receive on average 5.2 BEC scam emails.[2]

New technology, however, is also a target for attackers, and in late 2016 we saw the first major incident originating from IoT devices, the Mirai botnet, which was composed of routers, digital video cameras, and security cameras. Weak security – in the form of default and hard-coded passwords – made these devices easy pickings for attackers. After compromising millions of devices, the attackers controlled a botnet big enough to carry out the largest DDoS attacks ever seen. Just over a year ago the combined power of these compromised devices led to brief outages at some of the most popular websites and online services in the world. Mirai's impact was further magnified when the developer released the source code for the malware, which led to copycat efforts by other groups.[3]

Ransomware continues to plague businesses and consumers, and due to its destructiveness is one of the most dangerous cybercrime threats we now see. Criminal gangs engaged in indiscriminate campaigns involving massive volumes of malicious emails that in some cases overwhelmed organizations by the sheer volume of ransomware-laden emails alone. Attackers are demanding more and more from victims, and the average ransom demand *more than tripled* in 2016, from $294 to $1,077. The number of new ransomware families also more than tripled to 101, from 30 in both 2014 and 2015. The volume of attacks increased as well. Detections were up 36% percent from 2015, and by December we were seeing almost twice the daily volume that we observed in January.

---

[1] FBI Public Service Announcement, *Business E-mail Compromise – E-mail Account Compromise the 5 Billion Dollar Scam, May 4, 2017;* https://www.ic3.gov/media/2017/170504.aspx#fn3

[2] ISTR Email Threats 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf

[3] See *Symantec Internet Security Threat Report,* XX!!, April 2017 pp. 68

Ransomware has become a jack-of-all-trades tool for cybercriminals. Originally, criminals targeted primarily individual users with ransomware, trying to extract a few hundred dollars per victim. This continues to this day – and ransomware is an incredibly profitable venture for cybercriminals. Unfortunately, we have seen attackers using ransomware in other, more troubling ways. First, criminals are now using ransomware as part of sophisticated, multi-staged attacks on corporations that seek tens of thousands of dollars (or more) in ransom. Second, some destructive attacks have been disguised as ransomware – the malware encrypts crucial data on the victim's computer, effectively destroying it, and no decryption key is held by the attacker. So while it appears to be ransomware to the victim, the intent was always destruction because the attacker has no ability to decrypt the data. Finally, we are seeing groups linked to nation states using ransomware to steal funds – specifically, the Wannacry outbreak in May, which we linked to the Lazarus group.

II. Methods Attackers Use to Compromise Systems - Inside the Attacker's Tool Kit

Successful attacks share a common factor – a compromised device. From this one computer, attackers often are able to move within a system until they achieve their ultimate goal. But the threshold question is how do they get that foothold – how do they make that initial compromise that allows them to infiltrate a system?

We frequently hear about the sophistication of various attackers and about "Advance Persistent Threats" or "APTs," but the discussion of cyber attacks – and of cyber defense – often ignores the psychology of the exploit. Most attacks rely on social engineering – in the simplest of terms, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology.

Spear phishing, or customized, targeted emails containing malware, are still the most common form of attack. Attackers harvest publicly available information and use it to craft an email designed to dupe a specific victim or group of victims. The goal is to get victims to open a document or click on a link to a website that will then try to infect their computers. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many organizations and individuals do not have up-to-date security or properly patched operating systems or software. And many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach.

Social media is an increasingly valuable tool for cyber criminals in two different ways. First, it is particularly effective in direct attacks, as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to wonder if that feed may have been compromised or spoofed. Thus, attackers target social media accounts and then use them to "like" or otherwise promote a posting that contains a malicious link. But social media is also widely used to conduct reconnaissance for spear phishing or other highly targeted attacks as it often provides just the kind of personal details that a skilled attacker can use to get a victim to let his or her guard down.

One common web-based attack is known as a "watering hole" attack. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. They do so by compromising legitimate websites that their targets are likely to visit and modifying them so that they will surreptitiously try to infect visitors. For example, one attacker targeted mobile application developers by compromising a site that was popular with them. Cybercriminals gained control of these websites through many of the same tactics described above – spear phishing and other social engineering attacks on the site managers, developers, or owners. Many of these websites were compromised through

known attack vectors, meaning that good security practices could have prevented them from being compromised.

III. Protecting Against an Evolving Threat

Cybersecurity is about managing risk, whether at the individual or the organizational level. Assessing one's risk and developing a plan is essential. For the individual, the Federal Trade Commission's website is an excellent starting point for doing so.[4] The website provides educational resources for how to better protect your identity and privacy online as well as helpful tools to help you report and recover if your personal information is ever stolen. Similarly, we offer many tools and reference materials on our Norton and LifeLock websites.

For organizations of any size, the National Institute of Standards and Technology's Cyber Security Framework[5], developed by industry and government in 2014 and in which Symantec was an active contributor, provides a solid structure for risk management. It lays out five core cybersecurity functions (Identify, Protect, Detect, Respond and Recover) that all organizations can use to plan for managing cyber events and protecting against data breaches, as well as useful references to international standards. As detailed below, good security starts with the basics and includes measures specific to one's needs.

a. Protecting the Enterprise

Attacks are getting more sophisticated, but so too are security tools. Security still starts with basic measures such as strong passwords and up-to-date patch management. But while these steps may stop some older, simpler exploits, they will be little more than a speed bump for even a moderately sophisticated attack – and will do little to slow a determined, targeted attack.

Effective protection requires a modern security suite that is being fully utilized. An attack requires access, and attackers are increasingly relying on stolen credentials to gain their footholds. Deploying effective multi-factor authentication is essential to denying access to the would-be attacker. To block advanced threats and zero day attacks, sophisticated machine learning and advanced exploit detection and prevention technologies are necessary. This includes tools for detecting encrypted malware, as attackers are increasingly using encryption in an effort to bypass common security tools. Automated security tools learn how to identify attacks, even ones that have never been seen before. It is also increasingly critical to use big data analytics to evaluate global software patterns to create real-time intelligence. Today these analytics are able to identify and block entirely new attacks by evaluating how they are distributed and their relationships with other devices and other files.

Data protection is equally important, and a comprehensive security program includes data loss prevention (DLP) tools that index, track, and control the access to and movement of huge volumes of data across an organization. Perhaps most importantly, DLP tools will prevent that data from moving outside an organization. Organizations should also use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key.

Device-specific protections are also important. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. In the IoT world, there are authentication, encryption, and endpoint protection tools that are designed to run on

[4] http://www.consumer.ftc.gov/topics/privacy-identity
[5] http://www.nist.gov/cyberframework/

small and low power devices. These tools can protect everything from a connected vehicle to the small sensors built into a bridge or that monitor critical machinery.

Good security does not happen by accident – it requires planning and continued attention. But criminals will always be evolving, and security must as well.

b. Protecting the Individual

Consumers need to secure both their devices (computers, tablets, phones, anything "connected") and their identities. Device security used to be relatively simple –access and password management, patching and updating software, and employing modern security tools. These are still the pillars of good security, and there is significant overlap with the enterprise security steps laid out above. Individuals, like enterprises should employ multi-factor authentication whenever it is available, and in particular on financial or highly personal accounts. Individual security also includes caution when opening attachments, going to unknown links, or enabling macros in common software platforms. While this may seem like old news, the unfortunate reality is that criminals are always coming up with new ways to trick their victims into visiting a bad site, opening a malicious attachment, or otherwise unwittingly facilitating an attack.

The good news is that individuals *can* protect their computers and devices. Many scams directed at individuals take advantage of older, known vulnerabilities and tactics, and will not work on computers (or phones or tablets) that are updated and protected by modern security tools. Connected devices such add a new dimension to home security, but they too can be protected. First and foremost, consumers should make sure that they change any preset, default passwords on *anything* that connects to the internet. Finally, we all should stop and think before we purchase a connected device, or before we connect an internet-enabled device that we have purchased. Still, there will be some devices that simply cannot be secured – either because they lack the power to run security tools or because it is simply unavailable. For these home devices, we developed Norton Core™, the first router designed specifically to secure IoT devices, whether a connected appliance or a digital video recorder.[6]

Recent events have made clear, however, that individuals can be victimized by cyber criminals even if they have taken every possible step to protect their devices. And just as consumers can secure their devices, there are things that we all can do to protect ourselves against identity theft. A first step is to check your credit reports to look for accounts or activity that you do not recognize, which could indicate identity theft. You can do this for free by visiting annualcreditreport.com. Another option is to consider placing a fraud alert on your files, which warns creditors that you may be a victim of identity theft. If you do so, creditors are required to make a reasonable effort to verify that anyone seeking credit in your name is, in fact, you. You can also place a credit freeze on your credit files, which means that potential creditors cannot access your credit report. This makes it less likely an identity thief can open new accounts in your name. Finally, on a regular basis you should monitor your existing credit card and bank accounts and watch for charges or activity you do not recognize. The Federal Trade Commission offers other tips for protecting yourself after a data breach on its website.

Consumers can also obtain credit monitoring services and identity theft protection. Credit monitoring tracks changes to one or more your credit reports, including applications for a new credit card or a loan and can detect suspicious activity. Identity theft protection adds additional layers of protection, typically providing credit file monitoring at one or more of the three credit reporting agencies and sometimes a credit score from one agency or more. Services may include alerts if your personally identifiable information is used in ways that may not show up on your credit report such as commission

[6] *See https://us.norton.com/core*

of a crime or employment fraud. Identity theft protection may also provide restoration services that help victims resolve a variety of identity theft issues.

If you do believe that you are the victim of identity theft, you need to take action. Below are some steps to consider for some of the more common forms of identity theft:

1. If you spot unfamiliar transactions on a bank or credit card account, you could be the victim of **financial identity theft**. Contact your bank or credit card company immediately.
   - If someone has unauthorized access to your bank account, you will of course want to close that account and open a new one with a new account number. You will also want to work with the bank to resolve any fraudulent transactions.
   - If someone has stolen your credit card number, you should contact the issuer to alert them to the fraudulent charges and ask them to close the account and issue you a new card.
2. **Governmental identity theft** occurs when someone fraudulently shares your personal information with the government. One example is tax-related identity theft – for instance, an imposter uses your Social Security number and other personal information to file an income tax return in your name, hoping to obtain a fraudulent tax refund.
   - If you discover that you are a victim of tax-related identity theft, you will need to alert the IRS, the Federal Trade Commission and your local police department (you may need a police report to resolve the issue).
   - You should also contact one of the three major credit reporting agencies to place a "fraud alert" on your credit report, making it more difficult for criminals to open accounts in your name. The credit reporting agency you contact will contact the other two agencies.
   - The IRS also advises these additional steps:
     - Respond immediately to any IRS notice.
     - Complete the IRS Identity Theft Affidavit, Form 14039.

   Another example of governmental ID theft is employment fraud, when someone uses your Social Security number to obtain employment. If you are a victim of employment fraud, the Identity Theft Resource Center (ITRC) suggests that you file a police report and call the Social Security Administration (SSA) in your area. SSA forms can help you correct the fraudulent activity that is now part of your records. You will also need to inform the Internal Revenue Service and your state's internal revenue department, assuming you have a state income tax.

   And if someone is using your Social Security number for tax-related identity theft or employment fraud, they may also be using it for other purposes. It is a good idea to review your credit reports for any fraudulent activity.
3. It is possible also for an identity thief to assume your identity to see a doctor or visit an emergency room. This is called **medical identity theft**. Since your healthcare data could become mingled with your imposter's data, this crime could even threaten your health. The ITRC offers several recommendations, including:
   - Ask for copies of your medical records from the providers where your identity may have been used fraudulently.
   - Ask those same health care providers for a list of those with whom they have shared your protected health information – it may have the same errors.
   - Reach out to any medical facilities asking you for payment for services you did not receive. Tell them this is a case of identity theft or mistaken identity and ask what service was provided.

- File a police report in your local jurisdiction.

Unfortunately, there are numerous other types of identity fraud, and both the FTC and the ITRC provide resources and information for victims.

Conclusion

Citizens are increasingly aware of the cyber risk and the need to take precautions to secure their data and protect their privacy. While we cannot prevent every cyber attack or every data breach, applying cybersecurity best practices and using risk management principles to protect data appropriately can significantly reduce the attack surface and the impacts we see today. Every time someone patches a computer or mobile device, changes a password, or utilizes a modern security suite, he or she is making it more difficult for cybercriminals to operate. Like any other illicit activity, cybercrime will never be completely eliminated, but it can be fought – cybersecurity is a proverbial journey, not a destination. Understanding the threat, how it is changing, and where it is going, is essential if we are going to stay on track in this journey.

ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

November 1, 2017

The Honorable Bob Latta
Chairman
Digital Commerce and
Consumer Protection Subcommittee
2125 RHOB
Washington D.C. 20515

The Honorable Janice Schakowsky
Ranking Member
Digital Commerce and
Consumer Protection Subcommittee
2125 RHOB
Washington D.C. 20515

Re: Hearing on Securing Consumers' Credit Data in the Age of Digital Commerce

Dear Chairman Latta and Ranking Member Schakowsky:

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 35,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

There is very little doubt that Equifax's negligent security practices were a major contributing factor in the massive breach of 145.3 million Americans' most sensitive information. In the wake of the breach, EFF has the following policy suggestions for the subcommittee to consider in order to reduce the possibility of a future catastrophic breach and just as importantly, ensure that victims of these data breaches are made whole when a company is negligent with their sensitive data.

Congress Should Create a Victims Advocate to Assist Americans and Produce Empirical Data on the Financial Harms of Breaches

When almost half of the country has been victimized by a data breach, it's time for the federal government to begin devising a support structure for the victims. While the focus rightfully is on Equifax and it's negligent security, Congress should dedicating resources for victims. If a consumer's information is compromised, there is a complex process to wade through to figure out who to call and what kind of protections to place on one's credit information. A position should be created within the Executive branch and should be given the necessary prominence to direct federal resources for victim's assistance.

More importantly, this position would be in-charge of producing rigorous research reports on financial harms these data breaches inflict on the American public. This information will be critical federal courts have established a high bar for plaintiffs to sue negligent companies like Equifax. Under the *Spokeo* decision, the judiciary has effectively kept most data breach cases out of litigation because plaintiffs are not able to prove their harm in a

concrete manner[1]. Federal research and data analyzing the financial harm Americans have faced will help bridge that gap. If legal representation for victims can point to empirical data demonstrating that their clients have been harmed, then companies like Equifax will face the appropriate liability for their conduct and be held accountable for their failures to secure data.

Congress Should Avoid Creating New Criminal Laws

A kneejerk reaction to a significant breach like Equifax is to think that we need additional criminal laws aimed at those who are responsible. But the reality is, new criminal punishments would not have done anything to ensure that Equifax applies crucial security patches when they are available. This is because Equifax is solely at fault for the breach as they had ample opportunity to remedy the situation before it happened. Rather than expand criminal penalties Congress should incentivize protecting the data.

In our public interest litigation practice representing security testers, it is our experience that the laws that exist today hinder security researchers who wish to keep the public informed. For instance in Equifax's case, a security researcher had warned the company about its security vulnerabilities *months before* the actual breach happened; yet the company didn't do anything to fix them[2]. The security researcher couldn't go public with the findings without risking significant civil and criminal liability. Without a meaningful way for security testers to raise problems in a public setting, companies have little reason to keep up with the latest security practices and can use the law to suppress embarrassing disclosures. If Congress enhances or expands criminal penalties for unauthorized access under laws like the Computer Fraud and Abuse Act (CFAA), we'd all be worse for it. Rather, companies and the law should favor security audits by outside parties and publication of their findings to keep the public informed.

Protect Victims' Day in Court

As noted above, it is already a challenge for those seeking a remedy for data breach harms to get into court at all. For too many people impacted by data breaches, they learn to their great dismay that somewhere in the fine print of the agreement they had to click on or are otherwise subject to a waiver of their legal rights. While the mandatory arbitration clauses Equifax originally pursued received substantial negative press attention to pressure the

---

[1] Cindy Cohn & Amul Kalia, *Will Equifax Data Breach Finally Spur Courts (and Lawmakers) to Recognize Data Harms?*, DEEPLINKS BLOG, available at https://eff.org/deeplinks/2017/09/will-equifax-data-breach-finally-spur-courts-and-lawmakers-recognize-data-harms.

[2] Lorenzo Franseschi-Bicchierai, *Equifax Was Warned*, MOTHERBOARD, available at https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning.

company to desist, Congress should ensure that victims are entitled to all of their legal rights.

Prohibiting companies like Equifax from impairing any legal remedy in exchange for generally weak assistance like credit monitoring is essential given the scale of harm and likely repeat harms into the future. Failing to protect victims' ability to seek damages to their fullest will result in companies receiving a substantial windfall of reduced liability while inflicting catastrophic losses on the American public.

Congress Should Establish a Floor for Data Breach Laws

Any federal laws that are passed in response to data breaches should be the foundation upon which state's can build upon according to their needs. This would allow states to effectively update their laws and enforcement power on behalf of their citizens while yielding the extra benefit of assisting people that live in other states.

For example, California has one of the strongest data breach notification law in the country and EFF was actively engaged in its creation. Given the size of the state it effectively serves as a national notice system. By the time a company has to comply with California's law, the company has infrastructure in place to notify the rest of the country. States have a tendency to be capable of responding quickly to changing data collection practices and Congress should not pass a law that would gut their ability to do so.

Federal Trade Commission Needs to Have Rule-making Authority

Federal regulators have little power to ensure that entities like Equifax aren't negligent in their security practices. We rely on credit agencies to get essential services in our lives—apartments, mortgages, credit cards, just to name a few—yet the fact that they don't have to abide by a basic framework of standards to protect our sensitive information is detrimental to data security.

Congress needs to empower an expert agency like the Federal Trade Commission (FTC), which has a history and expertise in data security[3], by restoring its rule-making authority to set security standards and enforce them. FTC's current limitation to only get involved in matters of unfair dealing and deceptive conduct are inadequate to address the increasingly sophisticated technological landscape and collection of personal data by third parties.

---

[3] FEDERAL TRADE COMMISSION, *Data Security*, available at https://www.ftc.gov/datasecurity

ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

Create a Fiduciary Duty for Credit Bureaus to Protect Information

We live under a system where we need to rely on credit bureaus to execute even the most basic financial transactions. Very few of us chose to have our most sensitive information be hoarded by an entity like Equifax that we have no control over. Congress has the power to ensure that a credit bureau has special obligations and create a fiduciary duty for the bureaus to protect an individuals data. Without obligations to the individual to have adequate security practices, we will see more breaches on the scale of Equifax.

Free Credit Freezes, Not Credit Monitoring Services

It's become almost standard practice to offer data breach victims credit monitoring services. In reality, these services offer little protection to victims of data breaches[4]. Many of them are inadequate in the alerts they send consumers, and more fundamentally, there's little utility in being informed of improper usage of one's credit information *after* it's already been exploited. Consumers will still potentially have to spend hours to get their information cleared up with the various credit bureaus and entities where the information was used fraudulently. Instead, Congress should focus on ensuring that victims of data breaches get access to free credit freezes, which are much more effective in preventing financial harm to victims of data breaches.

We thank the subcommittee for holding this hearing and beginning the long process of investigating what happened and hopefully moving forward on legislation to improve the data security of all Americans. EFF stands ready support those efforts.

Sincerely,

Electronic Frontier Foundation

---

[4] KREBS ON SECURITY, *Are Credit Monitoring Services Worth it?*, available at https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 5, 2017

Mr. Francis Creighton
President and CEO
Consumer Data Industry Association
1090 Vermont Avenue, N.W., Suite 200
Washington, DC 20005

Dear Mr. Creighton:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on, Wednesday, November 1, 2017, to testify at the hearing entitled "Securing Consumers' Credit Data in the Age of Digital Commerce."

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

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, December 19, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

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

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

December 20, 2017

The Honorable Robert E. Latta
Chairman
Subcommittee on Digital Commerce & Consumer Protection
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Latta:

Thank you for the opportunity to appear before your subcommittee on November 1, 2017. In response to your December 5th letter, please find responses to additional questions from you and Congressman McKinley.

Please feel free to let me know if you have additional questions.

Sincerely,

[redacted]

Francis Creighton
President & CEO

Additional Questions for the Record
Francis Creighton, President & CEO
Consumer Data Industry Association

The Honorable Robert E. Latta

1. *What specific benefits do consumers see because of the personal and credit information that consumer reporting agencies (CRAs) collect and maintain in credit files?*
    a. *If CRAs did not collect and maintain such information on consumers, how would that impact the ability of banks, merchants, mortgage lenders, to name a few, to extend credit lines to consumers?*

Consumers benefit from the current system in a number of ways. The best place to start to understand the consumer benefits of consumer data on file with CRAs is what we call the "miracle of instant credit." When he was the chairman of the FTC, 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."

Chairman Muris went on to discuss the value of the FCRA in the marketplace. He said that "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]

Consumers benefit from being assessed based on their own personal credit histories. Today lenders are able to assess what product to offer a consumer based on her/his own history, accurately reflecting how s/he has handled credit in the past.

Consumers also benefit because the system today offers multiple efficiencies. Lenders do not have to require months of statements for every credit card or bank account before offering a loan product. Lenders can pull a credit report and have a comprehensive view of the consumer's history.

Because credit reports are always absorbing new information, a single missed payment is set in the context of years of on-time payments. Our credit reporting system allows for second chances for American consumers.

The US credit system contributes to the diversity of business model choices American banking consumers enjoy by providing disproportionate benefits to smaller financial institutions like community banks and credit unions, who have

[1] FTC Chairman Tim Muris, October 4, 2001 before the Privacy 2001 conference in Cleveland.

access to accurate and complete information on par with that available to very large banks. Our consumer credit system works whether you are at a global bank or a community-based credit union because companies share critical information across the system to benefit everyone.

Credit reports are also a check on human bias and assumptions. These reports provide lenders with a foundation of 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 consumers and safety and soundness of lending institutions – by ensuring the accuracy and completeness of information in consumer reports, and by providing businesses with the information they need to ensure consumers are treated fairly. Without this system, subjective judgements could be based on factors other than the facts of creditworthiness.

If CRAs did not collect and maintain consumer information consumers would no longer be able to be judged on their own personal histories. During the application process for new credit, financial institutions would be forced to attempt to ascertain a full picture of a borrower's current obligations. Lenders would have to present much more extensive applications and employ more people to review and confirm the information a consumer shares. In addition, because a lender would have no way of knowing whether the application presents a full and complete picture of a potential borrower's obligations, the lender would have to account for this increased risk by adding a premium to the rate being offered to the consumer. Consumers would have the burden of having to produce many more documents when being considered for a loan, and have to wait significantly longer as that information is confirmed. Ultimately, consumers would be forced to accept higher rates across the board. Consumers without significant accumulated assets would be the worst off, as companies would be likely more willing to lend based on assets available rather than on previous credit history.

2. *Please explain steps involved in how a credit check and credit report data are used by a CRA, a merchant, and a lender for example in the purchase or lease of an iPhone or another expensive consumer electronic device?*

The user in this situation is the retailer. In the case of the purchase of an expensive new personal device, the sale of the product is only part of the deal the consumer and the retailer are making. In this case a consumer is agreeing to a fixed term contract for service from a company, and the cost of the device is broken down over the course of the contract. So, for example, a $480 device may add $20 per month onto a four-year contract. But in effect, the retailer is letting someone walk out the door with a $480 device with no money down.

In this case a retailer, in effect, is extending credit to a consumer, in that the retailer is giving away a thing of value, only to have it paid back in monthly installments over a fixed term. Therefore, it is in a retailer's interest to see how this consumer has handled credit in the past. At the point of sale, after receiving personal information about a consumer, the retailer's computer system will access a credit report and determine whether someone can be extended credit and the terms if they are. This protects the retailer's investment in the consumer.

Reports have surfaced after the release of the new iPhone that some consumers who froze their credit after September 7th were not able to be among the first to sign up for the new devices as they failed to remove the freeze before visiting the store[2].

3. *Can the three major consumer reporting agencies—Experian, TransUnion, and Equifax—coordinate so that consumers only need to contact a single CRA to request a credit freeze on their credit file by all three CRAs?*

They are not able to do this at this time as each are required to individually authenticate consumers before freezing the report. Credit freezes laws vary from state to state and these differences drive state-by-state compliance. Unlike access to the annual free credit report under federal law, which allows national compliance and national coordination, the differences in state laws make national coordination and compliance impossible.

4. *Can a consumer request a credit freeze on their credit file by accessing a credit bureau's website, calling its toll-free telephone number, or mailing required documentation to the credit bureau via U.S. mail?*
    a. *How much time does it typically take for a credit freeze to take effect once a consumer requests such a freeze on their credit file?*
    b. *How much time does it typically take to thaw a credit freeze so a consumer to apply for credit or for any other financial transaction that requires third-party access to their credit file?*
    c. *Would a credit freeze mobile app allow consumers to instantaneously freeze and thaw access to their credit files?*

Nationwide CRAs are able to receive and act on requests, providing the consumer's information received is accurate and can be authenticated, via website, telephone of US Mail. Some state laws, however, dictate the process by which freezes must be placed. A uniform national standard on freezes would be preferable for all consumers.

---

[2] See, e.g. Associated Press: "Equifax breach could hit new iPhone buyers", September 15, 2017. https://www.cbsnews.com/news/equifax-breach-iphone-buyers-credit-freeze/ . Last accessed December 8, 2017

Once the request for a freeze placement, lifting, or removal is received and authenticated, action is taken, and often within minutes.

A mobile app for a credit freeze would only work if it allows for an ongoing relationship with a consumer. The reason why it can take time for a freeze to be set or lifted is because of requirements around authentication. Today, under state law, once a freeze is set, there is no further business relationship. However, having an app would suggest that the authentication credentials are stored in the app. Ensuring that this is the case requires a company to keep records and update them at all times. Today's system is PIN-based because that is the alternative authentication process.

5. *Can a consumer request a credit lock on their credit file by accessing a credit bureau's website, calling its toll-free telephone number, or mailing required documentation to the credit bureau via U.S. mail?*
    a. *How much time does it typically take for a credit lock to take effect once a consumer requests such a lock on their credit file?*
    b. *How much time does it typically take to unlock a credit lock so a consumer to apply for credit or for any other financial transaction that requires third-party access to their credit file?*
    c. *Would a credit lock mobile app allow consumers to instantaneously lock and unlock access to their credit files?*

The three nationwide CRAs are in different places on this important question. Since credit locks exist outside of state law, companies are able to be more flexible on what and how they offer these products.

TransUnion is currently the only company with a product on the market, and Equifax has announced that they will have a lock product available next year. Because of this, we can only address how TransUnion's lock product works.

For TransUnion's product, once the consumer has set up the system, the lock, unlock, thaw process happens very quickly, virtually instantaneously. This product is app-based and is designed to allow consumers to lock and unlock their files in real time at a point of sale. Equifax has announced that it will have a similar product available in early-2018.

6. *What is the process by which CRAs acquire credit report data?*
    a. *Please identify each of the specific types of data furnishers and suppliers that provide credit report data to the CRAs?*

CRAs have individual voluntary agreements with data furnishers, such as banks and other financial institutions, creditors, utilities, mobile phone carriers, and landlords. There are roughly 15,000 data furnishers.

7. *Why is it necessary for data furnishers, like creditors, to voluntarily supply personal and credit data and information to the CRAs?*
    a. *Are there government regulation or requirements that necessitate the constant supply of such data and information to maintain credit files?*

As noted in a seminal paper on credit data sharing[3],

> Comptroller of the Currency John Hawke, Jr. testified before Congress in 1999 that information exchanges serve a "useful and critical market function" that benefits consumers and businesses alike."[4] Consumer credit markets provide a case in point. The current U.S. economic boom has significantly raised the standard of living for U.S. citizens through the availability of over $5 trillion in outstanding mortgages and other consumer loans. Consumer credit finances homes and cars, funds college educations, and provides the credit cards that consumers use every day to purchase goods and services. The "almost universal reporting" of personal credit histories (under the rules of the Fair Credit Reporting Act) is, in the words of economist Walter Kitchenman, the "foundation" of consumer credit in the United States and a "secret ingredient of the U.S. economy's resilience."[5] Studies have shown that the comprehensive credit reporting environment in this country has given U.S. consumers access to more credit, from a greater variety of sources, more quickly, and at lower cost than consumers anywhere else in the world.[6]

Student loan servicers are required to report to credit bureaus by law (20 U.S. Code § 1080a). Fannie Mae and Freddie Mac guidelines require credit reporting. Federal banking regulators have strongly encouraged their regulated communities to participate in credit reporting. Non-bank furnishers of data, such as non-bank auto-lenders, landlords and others, participate in the system on a voluntary basis.

---

[3] Fred H. Cate, Michael E. Staten, The Value of Information-Sharing, The National Retail Federation's, Protecting Privacy in the New Millennium Series.

[4] Financial Privacy, Hearings before the Subcommittee on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of John D. Hawke, Jr.).

[5] Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns* 1 (The Tower Group 1999).

[6] John M. Barron and Michael E. Staten, "The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience," Credit Research Center, McDonough School Business, Georgetown University, February, 2000; Tullio Japelli and Marco Pagano, "Information Sharing, Lending and Defaults: Cross-Country Evidence," Working Paper No. 22, Centre for Studies in Economics and Finance, University of Salerno, May, 1999.

While the system is regulated through the Fair Credit Reporting Act, it is mainly a voluntary system where lenders take their sensitive customer information, and share it with a trusted third party, so that another financial institution – potentially a competitor—can access that information to make a better lending decision. Again, this is all done voluntarily, but within a significant regulatory structure. The resulting competition lowers prices to the consumer.

8. *What other specific data and information do consumer reporting agencies (CRAs) generate about U.S. consumers that are then supplied to other firms?*
    a. *Are CRAs using algorithms to compile enhanced profiles on U.S. consumers?*
    b. *Are data algorithms being utilized to credit new lines of business or business products for sale?*

CRAs are organized specifically as businesses that comply with the Fair Credit Reporting Act. Some CDIA members have additional business lines, which CDIA does not represent, that provide additional data brokerage services. Those data products are operated outside of the credit file. The credit file is kept entirely segregated and by law cannot be intermingled with these other businesses.

Credit scoring is another product that CDIA members provide as do other companies. The most famous version is FICO, which is not a CDIA member, though each of the nationwide CRAs provide scoring systems to a variety of lenders.

Different lenders have different needs. A long-term lender like a mortgage company might weigh certain facts in a credit report differently than a credit card lender as they are very different products. Therefore, they would likely use different soring systems. Our companies help businesses meet their risk management needs by customizing models for our customer's unique needs.

9. *What best practices or standardized requirements have CDIA and the CRAs implemented to protect personal and credit data at rest, in transit, and in process?*
    a. *Is encryption part of any CDIA best practices?*

CDIA members have implemented their own best practices to protect their systems. They are also regulated by state and federal law to ensure the highest level of protection. My written testimony goes into significant detail outlining the different requirements and standards to which CDIA member companies must live up.

CDIA does not maintain a best-practices program.

10. What best practices or standardized requirements have CDIA and the CRAs implemented for post-breach notification and consumer protection remediation to consumer affected?

CDIA does not maintain a best-practices program, but our members spend a lot of financial and personnel resources to develop systems to protect data and to protect consumers, all of which are done with legal compliance as the benchmark.

11. Since 2012, the CFPB has subjected the larger CRA entities to agency supervision. Prior to 2012, that wasn't the case. Explain how CPFB supervision covers information security matters and might have prevented the Equifax breach.

CFPB supervision does not extend to data security. Congress specifically designated credit reporting agencies as financial institutions that are subject to the information security requirements of the Gramm-Leach-Bliley Act (GLBA), in 1999, and its implementing regulation, the Standards for Safeguarding Customer Information ("Safeguards Rule") promulgated by the Federal Trade Commission (FTC).

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 any customer information at issue. The common-sense provisions of the Safeguards Rule are general parameters designed to allow evolving standards to keep pace with the evolving threat landscape. At their inception lawmakers and regulators anticipated that private institutions and the government overseers closest to the battle lines and with the greatest expertise in these matters would fine-tune industry best practices over time.

The Honorable David McKinley

1. What is the <u>one</u> most important thing companies like Equifax should do to enhance our confidence in their ability to keep sensitive data secure?

Businesses that hold personal information must continue to organize their companies, governance, and investments with security as the highest business goal, not an afterthought when designing a new product.

2. What is the <u>one</u> most important thing Congress should do?

Congress should require the executive branch to vigorously pursue hackers and hold them accountable to the same kinds of justice to which we hold other international criminals.

3. *How long does it take to freeze or thaw a credit freeze? Is it instantaneous? If it's longer than a few minutes or hours, would a mobile app make it instantaneous?*

Nationwide CRAs are able to receive and act on requests, providing the information received is accurate and can be authenticated, via website, telephone of US Mail. Some state laws, however, dictate the process by which freezes must be placed. A uniform national standard on freezes would be preferable for all consumers.

Once the request for the placement, lifting, or removal of a freeze is received and authenticated, action is taken, often with minutes.

A mobile app for a credit freeze would only work if it allows for an ongoing relationship with a consumer. The reason why it can take time for a freeze to be set or lifted is because of requirements around authentication. Today, under state law, once a freeze is set, there is no further business relationship. However, having an app would suggest that the authentication credentials are stored in the app. Ensuring that this is the case requires a company to keep records and update them at all times. Today's system is PIN-based because that is the alternative authentication process.

4. *Can consumers freeze and lock their Equifax account simultaneously?*

Not at this time. Equifax's lock system has not come on line yet and until it does we do not know precisely what features will be available.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 5, 2017

Mr. James Norton
Adjunct Lecturer
Johns Hopkins University Zanvyll Krieger School of Arts and Sciences
1717 Massachusetts Avenue, N.W.
Washington, DC 20036

Dear Mr. Norton:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on, Wednesday, November 1, 2017, to testify at the hearing entitled "Securing Consumers' Credit Data in the Age of Digital Commerce."

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

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, December 19, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

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

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Securing Consumers' Credit Data in the Age of Digital Commerce

U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

James Norton – QFR Answers

December 19, 2017

Questions from the Honorable David McKinley of West Virginia:

1. **What is the one most important thing companies like Equifax should do to enhance our confidence in their ability to keep sensitive data secure?**

   While there is no single policy or practice that will effectively ensure data security in all cases, I believe that, generally, companies like Equifax could enhance public confidence by providing greater transparency regarding their cybersecurity efforts – including whether they have established an executive level position within the company charged with developing and implementing security practices across the business. The executive would not be a lone ranger but would have the resources and authority across the business, with daily access to the CEO and senior government officials to work proactively to stay ahead of emerging cyber threats and safeguard sensitive data.

2. **What is the one most important thing Congress should do?**

   Congress should provide the necessary appropriation to enable and build a cyber infrastructure within Federal, state and local governments to establish them as reliable resource for the private sector. Too many companies lack the requisite expertise and resources to effectively tackle rapidly evolving cyber threats. Since the Federal Government as well as state and locals are dealing with many of the same challenges, they are well positioned to identify best practices (including by convening public and private stakeholders) and provide technical assistance. However, to date, cyber functions within the government have been under-resourced and tasked with overly broad mandates that leave little capacity for them to serve this critical leadership role for the private sector.

3. **Is social media becoming an increasingly effective tool for cyber criminals? In September after Equifax publicly disclosed the breach, Equifax repeatedly tweeted the wrong URL for its consumer protection website. Is that an example of cyber-criminal exploiting social media for nefarious purposes?**

   While I cannot comment about what may have caused Equifax to tweet the wrong link, I believe it is accurate to say that bad actors are making increasing use of social media, as a way to both spread malware and access

personal data. Consumers should be cognizant about sharing personally-identifiable information (like addresses, birth dates, and telephone numbers) on social media platforms and should be cautious when clicking on suspicious links, even those that have apparently been shared by known parties.

4. What kind of new data security developments should CEOs, Chief Information Security Officers, and Chief Information Officers and indeed everyone be aware of?

In today's complex cyber environment, threats are changing rapidly, so it is imperative that company executives – especially those in charge of sensitive personal data – remain aware of the most up-do-date, effective security solutions. However, companies and individuals can also take additional simple, effective steps to improve data security. Companies must be diligent about training employees on their role in keeping information protected — with an emphasis on recognizing phishing and spear phishing emails that are designed to trick them into giving away credentials or installing malware. Training should also cover smart social media practices, ground rules for downloading software, and the importance of strong passwords. For individuals, comparatively simple steps – like regularly changing passwords and ensuring that security software is up to date – can meaningfully reduce the vulnerability of personal devices to cyber attacks.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 5, 2017

Mr. Bruce Schneier
Adjunct Lecturer in Public Policy
Harvard Kennedy School
75 Binney Street, Floor 3
Cambridge, MA 02142

Dear Mr. Schneier:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on, Wednesday, November 1, 2017, to testify at the hearing entitled "Securing Consumers' Credit Data in the Age of Digital Commerce."

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

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, December 19, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

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

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

[Mr. Schneier did not answer submitted questions for the record by the time of printing.]

Additional Questions for the Record

The Honorable Jan Schakowsky

1. At the hearing, you recommended that Congress move forward with legislation that makes credit freezes the default for consumers. Instead of credit freezes, some consumer reporting agencies (CRAs) are offering free credit locks, and they are encouraging consumers to use the lock. What is stopping these CRAs from implementing the credit freeze as the default setting for consumers?

2. In your written testimony for the hearing, you stated that the financial markets actually reward bad behavior. Please expand on this idea.

3. According to the Privacy Rights Clearinghouse, more than 1 billion records have been exposed in data breaches reported in the United States since 2005. But the total population of the United States is about 323.1 million.

    a. Do you agree that this disparity would indicate that the personal information of many Americans has been breached multiple times?

    b. Your written testimony mentioned that "current law is too narrowly focused on people who have suffered financial losses directly traceable to a specific breach." How often are individual victims actually able to prove that they have suffered damages resulting from a specific breach?

    c. Given that most Americans have been the victims of multiple breaches, do you agree that that current law is not working for most victims?

4. What recourse, if any, do consumers have against the companies that failed to adequately protect their personal information?

5. Do companies that fail to protect consumers' personal information face any penalties at the federal level, particularly if the data breached is not from a consumer report but a different database?

6. The recent Equifax breach brought new attention to the consumer reporting industry and CRAs. But I am not convinced that consumers understand that these companies are also data brokers. I am also not convinced that consumers understand how these companies collect data.

    a. How many consumer reporting agencies are there that collect information on Americans?

    b. How many data brokers are there?

    c. Can you confirm that the three largest consumer reporting agencies, including Equifax, are also data brokers?

7. Although consumers have the right to free credit reports from each of the three major credit reporting agencies once each year, that report does not include all the information that these companies hold on each consumer. Is that right?

8. Mr. Creighton testified that the U.S. has "a credit system that other nations seek to emulate: a detailed regulatory regime that limits the sharing of information for permissible purposes only and strict requirements on accuracy, consumer access and correction." But those regulations, to the extent they are effective, do not apply to data brokers, including consumer reporting agencies, when they collect, share, and sell information that is not a consumer report as defined by statute. And most data brokers do not allow consumers to access and edit the information about them or opt-out of its marketing services.

    a. Should consumers be able to access the information that brokers hold about them? Why or why not?

    b. Should consumers have the right to dispute inaccurate information that brokers hold about them? Is it important that they have that right? Why or why not?

9. In the testimony submitted by Jeff Greene of Symantec, he mentioned a few types of identity theft. In addition to financial identity theft, he talked about government identity theft such as tax-related identity theft; medical identity theft such as when a person uses your identity to get medical attention; and others.

    a. Does identity theft always result in economic losses for the person whose identity was stolen?

    b. Is identity theft the only consequence of a data breach for consumers?

10. It is also important to note that blocking access to your credit report, through freezes or locks, would not stop all the potential repercussions that consumers face after a breach, including the various types of identity theft. Neither the typical credit monitoring services, especially those limited to one year, nor the credit lock services will help consumers protect themselves from non-credit effects of a breach. Even credit freezes will not help with everything. What can we do to help consumers after a breach?

11. Do data brokers also collect information about consumers' financial decisions? What other kinds of information do they collect?

12. Is it possible that the information that data brokers collect and sell could affect the products and services that individual consumers are offered, or the prices they are charged?

13. After multiple hearings on this subject, it appears that there is no way for consumers to completely opt out of having their personal information collected by either CRAs or data brokers. Is this accurate?

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 5, 2017

Ms. Anne P. Fortney, Esq.
Partner Emeritus
Hudson Cook, LLP
1909 K Street, N.W., 4th Floor
Washington, DC 20006

Dear Ms. Fortney:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on, Wednesday, November 1, 2017, to testify at the hearing entitled "Securing Consumers' Credit Data in the Age of Digital Commerce."

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

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, December 19, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

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

Sincerely,

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Responses to Additional Questions for the Record

Questions from the Honorable Robert E. Latta:

Question 1. What regulations currently exist that require CRAs to put in place reasonable practices to protect against cyber-attacks?

Response: As explained in my Prepared Statement, the security and confidentiality requirements of the Gramm-Leach Bliley Act ("GLBA") apply to "financial institutions," a term which is broadly defined to include consumer reporting agencies ("CRAs"). The Federal Trade Commission's Safeguards Rule, 16 C.F.R §§ 314.1 *et seq.*, which implements the GLBA's data security requirements, applies also to CRAs.

The Safeguards Rule establishes the standards for "developing, implementing, and maintaining reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of customer information."[1] The Rule makes clear that these standards apply to "any record" containing "nonpublic personal information," another term that is very broadly defined, about a customer that is handled or maintained by the financial institution or its affiliates.[2]

Because the risks encountered by financial institutions, including CRAs, vary with the types of products and services they provide to consumers, the Safeguards Rule imposes a compliance requirement that takes into account the "nature and scope" of the financial institution's activities as well as the "sensitivity of any customer information" that is handled or maintained.[3] That is, the Rule provides a rigorous standard that is designed to be flexible depending upon the identified risks presented by the financial institution's specific business and the types of data received and maintained. Understanding that this obligation is risk-based is critical to recognizing the valuable role the Rule plays in ensuring that customer information is adequately protected.

To meet the Safeguard Rule's standards, a financial institution's written Information Security Program ("ISP") must:

1. Ensure the security and confidentiality of customer 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.[4]

The written ISP must include a number of required elements designed to ensure that the above-identified objectives are met. These include the following:

1. That one or more employees be specifically designated to coordinate the ISP;

[1] 16 C.F.R. § 314.1.
[2] 16 C.F.R. § 314.2(b).
[3] 16 C.F.R. § 314.3(a).
[4] 16 C.F.R. § 313.3(b).

2. That a risk assessment be completed to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the customer information handled or maintained. Part of this risk assessment must also include the consideration of how the financial institution will detect, prevent and respond to attacks, intrusions and other events that compromise the security of the system;

3. That the implemented safeguards be designed to address the risks identified through the risk assessment. That these safeguards are adequate is ensured by the requirement that the safeguards be regularly tested and monitored to ensure their effectiveness;

4. That any service providers used by the financial institution be overseen to ensure that they too take the steps required to safeguard any customer information that is entrusted to them or that they receive or maintain on behalf of the financial institution; and

5. That the ISP be regularly evaluated and adjusted in light of the results of the required ongoing testing and monitoring to ensure the ISP's continued effectiveness.[5]

The above summarizes just the Safeguard Rule's protections. The Fair Credit Reporting Act ("FCRA") includes its own protections governing the confidentiality of consumer information. For example, the FCRA protects against unauthorized access to consumer report information by imposing the following requirements:

1. CRAs must maintain reasonable procedures to limit the release of consumer report information to only those persons who have a statutorily defined "permissible purpose" to obtain such information; [6]

2. CRAs must require that any person seeking to obtain consumer report information identify themselves, certify the permissible purpose for which the information is sought and certify that the information will be used for no other purpose;[7]

3. CRAs must maintain reasonable procedures to verify the identity of the person seeking the consumer report information and the existence of the permissible purpose certified by the person; [8] and

---

[5] 16 C.F.R. § 314.4. More information about these requirements may be found on the FTC website: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.
[6] 15 U.S.C. §§ 1681b(a), 1681e(a).
[7] 15 U.S.C. § 1681e(a).
[8] *Id.*

Responses to Additional Questions for the Record

4. CRAs must keep accurate records of every person who receives a consumer report on a particular consumer and, upon the consumer's request, disclose that information to the consumer.[9]

The above FCRA provisions protect consumer report information in two-ways. First, they ensure that only authorized recipients receive the information. Second, they ensure that consumers are able to monitor who receives their information.

In addition to the protections identified above, both the FTC and the Consumer Financial Protection Bureau ("CFPB") have used their authority to bring enforcement actions when data security violations have been identified.

The FTC uses its authority under Section 5 of the FTC Act to pursue companies that misrepresent their data security practices or that lack adequate data security measures.[10] Since 2001, the FTC has used this authority to bring enforcement actions and obtain settlements in approximately 60 cases against businesses that the FTC charged with failing to provide reasonable and appropriate protections for consumer information. [11]

Similarly, the CFPB has used its authority under the Consumer Financial Protection Act ("CFPA") to pursue actions against entities within its enforcement jurisdiction when they commit unfair, deceptive or abusive practices.[12] The CFPB used this authority to obtain civil penalties in the data security context from a company that allegedly deceived consumers concerning the company's data security practices and the security of the company's online payment platform.[13]

---

[9] 15 U.S.C. § 1681g(a)(3).

[10] Section 5 prohibits unfair or deceptive acts or practices and provides that an act or practice is unfair if the act or practice (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(a) and (n). *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), *available at* https://fas.org/sgp/crs/misc/R43723.pdf.

[11] FEDERAL TRADE COMMISSION, "Prepared Statement of the Federal Trade Commission on Small Business Cybersecurity: Federal Resources and Coordination Before the Committee on Small Business" (March 8, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1174903/p072104_commission_testimony.pdf.

[12] 12 U.S.C. §§ 5536(a)(1)(b), 5565(c).

[13] CONSUMER FINANCIAL PROTECTION BUREAU, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices" (March 2, 2016) *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

Responses to Additional Questions for the Record

Question 1a. Are there any specific gaps in regulation that led to the Equifax breach or was that the result of Equifax simply not doing what they were required to do?

Response: I have not been in a position to investigate the circumstances leading to the Equifax security incident. Rather, my knowledge of the incident is limited to what has been publicly reported in the media and the information available through Equifax's website.[14]

Based on this information, it does not appear that there are gaps in regulation that led to the incident. Moreover, the fact of a breach alone does not establish that the company which was the subject of the breach violated the law. Federal and state regulators recognize that there is no such thing as perfect data security:

> Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[15]

As was explained in response to Question 1, the existing regulatory framework already includes stringent requirements that a CRA protect the security and confidentiality of consumer information. Based on media reports, it appears that Equifax detected the breach, investigated its cause, took steps to stop the breach, notified law enforcement, notified affected consumers who were entitled to direct notice and offered all affected consumers additional tools to protect their identity.[16]

The GLBA and its implementing Safeguards Rule reflect a Congressional and Regulatory balancing of interests between (a) protecting consumer information and (b) ensuring that consumer information is available for limited use and disclosure by financial institutions that provide important products and services to consumers. There are tens-of-thousands of such financial institutions in the U.S. That significant data breaches are so rare that when they occur they draw national media attention is a strong indication that Congress and the FTC have struck the correct balance.

Because my knowledge of the Equifax breach is limited to what is publicly available, I can't comment further on what Equifax may or may not have done prior to the incident.

---

[14] *See,* Cybersecurity Incident & Important Consumer Information, available at https://www.equifaxsecurity2017.com/.

[15] *Commission Statement Marking the FTC's 50th Data Security Settlement*, Federal Trade Commission, Jan. 31, 2014, available at https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[16] *See,* Cybersecurity Incident & Important Consumer Information, available at https://www.equifaxsecurity2017.com/frequently-asked-questions/

Responses to Additional Questions for the Record

Question 2. Would extending the existing data security requirements for financial institutions to credit bureaus and other companies that sell credit reports have a meaningful mitigating effect on future data breaches?

Response: As noted in my response to Question 1 above, the FTC's Safeguards Rule already applies to consumer reporting agencies ("CRAs"). The FTC Rule is similar to the Interagency Guidelines Establishing Standards for Safeguarding Customer Information that apply to institutions supervised by the federal financial institution regulatory agencies (the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency). Both the FTC Rule and the Interagency Guidelines were mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999, and both the Rule and the Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of nonpublic personal information.

In addition, as noted in connection with the more than 60 enforcement actions pursued by the FTC against companies who failed to provide adequate protections for consumer information, federal regulators already have strong available tools for ensuring that consumer report information and other information on consumers is protected by applicable law.[17]

Question 3. What are the Gramm-Leach-Bliley Act consumer protection provisions in force today to ensure financial institutions, like the CRAs, protect consumer's financial information?

Response: Please see my response to Question 1 which outlines the protections available under the FTC's Safeguards Rule, implementing the Gramm-Leach Bliley Act ("GLBA").

Question 4. What are the Fair Credit Reporting Act consumer protection provisions in force today to ensure financial institutions, like the CRAs, protect consumer's financial information?

Response: Please see my response to Question 1 which outlines some of the protections available under the Fair Credit Reporting Act ("FCRA"). Moreover, the FCRA requires that "consumer information," which is any information that is a consumer report or is derived from a consumer report, be disposed of a manner that "protects against unauthorized access to or use of the information...."[18] In addition, the FCRA imposes upon financial institutions and other creditors the obligation to develop and implement identity theft protection programs that are "appropriate to the size and complexity of the financial institution or creditor and the nature

[17] FEDERAL TRADE COMMISSION, "Prepared Statement of the Federal Trade Commission on Small Business Cybersecurity: Federal Resources and Coordination Before the Committee on Small Business" (March 8, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1174903/p072104_commission_testimony.pdf.

[18] 15 U.S.C. § 1681w(a); 16 C.F.R. § 682.3.

and scope of its activities."[19] The program must include policies and procedures for responding to security incidents that result in unauthorized access to customer account information held by the financial institution or creditor.[20]

The FCRA also includes provisions which protect consumer information from misuse and provide consumers with powerful tools for protecting themselves from identity theft. These include:

1. The financial institution's obligation to respond to information requests from victims of identity theft by providing the consumer, who provides proper identification, with the business transaction records resulting from the alleged identity theft;[21]

2. The financial institution's obligation to reconcile address discrepancies between the user's file information maintained by the CRA and the address information the user receives from the consumer;[22]

3. The consumer's ability to place fraud alerts in their consumer report file which prohibit the recipients of consumer reports containing such alerts from establishing new accounts or extending credit without first using procedures that are designed to allow the user to form a reasonable belief that it knows the identity of the consumer requesting the credit;[23]

4. The consumer's ability to request that the CRA block the furnishing in a consumer report of any information the consumer identifies as resulting from identity theft;[24] and

5. Limiting the printing of a consumer's credit card number on an electronically printed receipt to just the last 5 digits of the number.[25]

Question 4a. **Under the Fair Credit Reporting Act, a consumer reporting agency may divulge a consumer report only under certain, enumerated conditions, "and no other." In your opinion, would it be a violation of this provision for a credit reporting agency to allow cyber-criminals to access a person's credit report?**

Response: Because a consumer reporting agency's ("CRA's") business depends upon the integrity of the information in its consumer reporting databases, it is inconceivable that it would "allow" a cyber-criminal to access its information systems to obtain a person's consumer

[19] 16 C.F.R. § 681.1(d).
[20] 16 C.F.R. Pt. 681, App. A, Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation.
[21] 15 U.S.C. § 1681g(e).
[22] 15 U.S.C. § 1681c(h); 16 C.F.R. § 641.1
[23] 15 U.S.C. § 1681c-1(h).
[24] 15 U.S.C. § 1681c-2(a).
[25] 15 U.S.C. § 1681c(g).

report. As noted in my response to Question 1, the FCRA requires CRAs to maintain reasonable procedures designed to limit the furnishing of consumer reports to the one of the statutorily defined "permissible purposes." These procedures must require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. In addition, every CRA must make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing a consumer report. No CRA may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a "permissible purpose."[26] If a CRA follows these requirements in providing a consumer report, it should not be liable under the FCRA, even if the user of that report lacks a permissible purpose.

If a CRA failed to have reasonable procedures to avoid providing a consumer report to a person, including a cyber-criminal, that lacked a "permissible purpose," the CRA could be liable under the FCRA. However, if a CRA had insufficient information security safeguards and those deficient safeguards provided a means by which a cyber-criminal could access the information maintained by the CRA for consumer reporting purposes, such a deficient Information Security Program ("ISP") would not be a violation of the FCRA's permissible purpose provisions, but could be a violation of the Safeguards Rule (discussed in response to Question 1 above).

Question 5. Under the Dodd Frank Act, the Consumer Credit Protection Bureau was given authority to supervise the CRAs. Would that authority have allowed CFPB to direct the CRAs to take steps to ensure they did not allow unauthorized access to individual credit reports?

Response: The CFPB has supervisory authority over nationwide CRAs with respect to their compliance with certain enumerated consumer financial laws, including the FCRA and CFPA's prohibitions against engaging in unfair, deceptive, or abusive acts and practices.

The CFPB's Examination Procedures for CRAs that are larger participants makes clear that the CFPB has the authority to examine CRAs to determine their compliance with the FCRA's permissible purpose provisions.[27] It also makes clear that this examination process is very detailed, requiring the CRAs to respond to multiple requests for information and documents. These requests are all intended to assess whether the CRAs have the required policies and procedures in place to ensure that consumer report information is only released to those users who have a permissible purpose, have certified that permissible purpose to the CRAs, and for whom the CRAs have completed the process of verifying both the identity of the user and the validity of the certified permissible purpose.[28]

---

[26] 15 U.S.C. §§ 1681b(a), 1681e(a).
[27] *See,* CFPB Examination Procedures, Consumer Reporting Larger Participants at Procedures 16-19, available at http://files.consumerfinance.gov/f/201209_cfpb_Consumer_Reporting_Examination_Procedures.pdf.
[28] *Id.*

The result of a CFPB examination process could be a report that identifies discrepancies in the CRA's compliance policies and procedures and imposes requirements upon the CRA to address such discrepancies.

Question 6. Is the regulatory framework for CRA sufficient to protect U.S. consumers from data security and privacy concerns?

Response: Yes, as explained in the specific response to Question 1, and more generally above, a number of existing laws already provide robust protections for consumer report information maintained by the CRAs.

Question 7. Could Congress authorize Consumer Financial Protection Bureau to examine CRAs for adherence to the Safeguards Rule?

Response: Yes, but in the Dodd Frank Act, Congress continued to vest the FTC with the authority to enforce the Safeguards Rule. This seemed appropriate at the time, and continues to seem appropriate given the FTC's developed expertise in the area of data security. In addition to its Safeguards Rule enforcement authority, the FTC retains authority to enforce the FCRA's Disposal Rule, which requires that companies dispose of consumer report information properly in a way that "protect[s] against unauthorized access to or use of the information...."[29]

Question 8. Could Congress provide the Federal Trade Commission with civil penalties against CRAs for failure to adhere to the Safeguards Rule?

Response: The FTC's principal tool for the enforcement of the Safeguards Rule is to bring enforcement actions to stop law violations and to require companies to take affirmative steps to remediate unlawful behavior. The FTC may require, when appropriate, implementation of comprehensive privacy and information security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule.

[29] 16 C.F.R. § 682.3(a).

Responses to Additional Questions for the Record

Questions from the Honorable David McKinley

Question 1. What is the one most important thing companies like Equifax should do to enhance our confidence in their ability to keep sensitive data secure?

Response: I've not been in a position to investigate the Equifax response to its security incident. So, it is unclear to me whether Equifax could have done more than it did when the security incident was identified. Based on published reports, it appears that Equifax detected the breach, investigated its cause, took steps to stop the breach, notified law enforcement, notified affected consumers who were entitled to direct notice and offered all affected consumers additional tools to protect their identity.[30] From these reports, it appears that Equifax took multiple steps that should enhance Congressional and public confidence that CRAs are able to secure sensitive data. These are also the steps required by existing law, as explained in my detailed responses to questions 1 and 4 above.

Question 2. What is the one most important thing Congress should do?

Response: At this time, there is no national standard for when and how companies should notify consumers of data breaches. The FTC has recommended that Congress enact a federal law that would require companies, in appropriate circumstances, to notify consumers when there is a security breach. Although most states have breach notification laws, a consistent national requirement would ensure that all consumers are notified of a security breach when the incident meets a single test, defined by Congress.

Question 3. I know there are 100s of credit bureaus, but do the three major bureaus maintain an effective monopoly on the supply of credit reports?

Response: No, the existing nationwide CRAs do not maintain an effective monopoly. The reason there are so few nationwide CRAs is that the financial and technological resources necessary to comply with the myriad of federal and state laws governing the collection, maintenance, and release of consumer report information are so great that only very large corporations can afford them. This is an economic barrier to entry to becoming a nationwide CRA that is a direct result of the highly-regulated CRA marketplace.

[30] *See*, Cybersecurity Incident & Important Consumer Information, available at https://www.equifaxsecurity2017.com/frequently-asked-questions/.

Responses to Additional Questions for the Record

Question 4. The CFPB has broad authority to bring enforcement case for unfair and deceptive business practices. Are you aware of any CFPB enforcement cases concerning information security using the unfair and deceptive standard?

Response: As the question notes, the CFPA authorizes the CFPB to seek civil penalties in connection with UDAAP violations for those entities within the CFPB's jurisdiction.[31] The CFPB has used this civil penalty authority in the data security context. In an action against a company for allegedly deceiving consumers about the company's data security procedures and the security of the company's online payment platform, the CFPB required the company to enact comprehensive data security measures (including a data security risk assessment and audit program). In addition, the company was required to train its employees on the company's data security policies and procedures, including on how to protect consumers' sensitive personal information. The company was also required to pay a civil money penalty for its alleged violations.[32]

Question 4a. Do you understand the Dodd-Frank Act to prevent information security enforcement, even under the broad unfairness and deception standards?

Response: No, that is not my understanding. The enforcement action referred to in response to Question 4 above is an example of the CFPB using this UDAAP authority in connection in the context of an enforcement action dealing with information security.

[31] 12 U.S.C. §§ 5536(a)(1)(b), 5565(c).

[32] CONSUMER FINANCIAL PROTECTION BUREAU, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices" (March 2, 2016) *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.