RPTR PETERS

EDTR HOFSTAD

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, D.C.

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

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

Also Present: Representatives Barton, Cramer, and Duncan.

Staff Present: Kelly Collins, Staff Assistant; Zachary 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, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Katie McKeogh, Press Assistant; 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.

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 vulnerability 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.

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

[The prepared statement of Mr. Latta follows:]

******** COMMITTEE INSERT ********

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.

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.

[The prepared statement of Ms. Schakowsky follows:]

******** COMMITTEE INSERT ********

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.

The Chairman. 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.

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

[The prepared statement of The Chairman follows:]

******** COMMITTEE INSERT ********

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.

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 individuals' 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.

I yield the remainder of my time to Congresswoman Matsui.

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

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.

[The prepared statement of Ms. Matsui follows:]

******** COMMITTEE INSERT ********

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 CEO, CONSUMER DATA INDUSTRY ASSOCIATION; JAMES NORTON, ADJUNCT LECTURER, JOHNS HOPKINS UNIVERSITY ZANVYLL KRIEGER SCHOOL OF ARTS AND SCIENCES; BRUCE SCHNEIER, ADJUNCT LECTURER IN PUBLIC POLICY, HARVARD KENNEDY 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:]

******** INSERT 1-1 ********

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, D.C. 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:]

******** INSERT 1-2 ********

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. Okay.

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 explain -- 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 okay. 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 because 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:]

******** INSERT 1-3 ********

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. Here is 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:]

******** INSERT 1-4 ********

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. Okay, 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 lots 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 have 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. -- 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.

RPTR TELL

EDTR HOFSTAD

[11:30 a.m.]

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. Okay. 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. Yeah, 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. Okay. 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. Cardenas. 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 -- "Schneier"?

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

Mr. Cardenas. Okay. "Schneier." Okay. 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. Cardenas. 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 what -- I mean, want 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. Cardenas. 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. Cardenas. 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. Cardenas. 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. Cardenas. Okay.

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. Yeah. 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 any 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. Okay. I beg your pardon.

Mr. Creighton. But, yeah, and those are coming on line 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. Okay. 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. Yeah. 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. Okay.

Mr. Schneier. -- that the world is moving that way. Europe is turning into the regulatory powerhouse --

Ms. Matsui. Sure.

Mr. Schneier. -- and they are going to be leading us more and

more.

Ms. Matsui. Because we are reacting more than --

Mr. Schneier. Yeah. 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. Okay.

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. Okay.

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

Ms. Matsui. Okay.

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 information. 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 bureaus. 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, okay?

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. Okay. 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. -- 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. Yeah, 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. Okay. 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. Okay.

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. Okay.

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. Yeah. 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. Yeah, 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 business is an important step and just saying, okay, 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, okay, 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 out-years and starting to develop a strategy of, okay, 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. Okay.

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

RPTR PETERS

EDTR HOFSTAD

[12:28 p.m.]

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. Okay. 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. Yeah, 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, yeah, 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. Okay.

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. Okay. 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. Okay.

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. Okay. 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. Yeah, good luck figuring out how.

Ms. Schakowsky. I am sorry?

Mr. Schneier. Good luck figuring out how.

Ms. Schakowsky. Yeah. 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. Okay. 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 were 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. Okay.

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 prepared statement of Mr. Greene follows:]

******** INSERT 3-1 ********

[The letter follows:]

******** COMMITTEE INSERT ********

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.]