IMPROVING DATA SECURITY AT CONSUMER REPORTING AGENCIES

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC AND CONSUMER POLICY

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

March 26, 2019

Serial No. 116–12

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
http://www.oversight.house.gov or
http://www.docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

36–064 PDF WASHINGTON : 2019

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Harley Rouda, California
Katie Hill, California
Debbie Wasserman Schultz, Florida
John P. Sarbanes, Maryland
Peter Welch, Vermont
Jackie Speier, California
Robin L. Kelly, Illinois
Mark DeSaulnier, California
Brenda L. Lawrence, Michigan
Stacey E. Plaskett, Virgin Islands
Ro Khanna, California
Jimmy Gomez, California
Alexandria Ocasio-Cortez, New York
Ayanna Pressley, Massachusetts
Rashida Tlaib, Michigan

Jim Jordan, Ohio, *Ranking Minority Member*
Justin Amash, Michigan
Paul A. Gosar, Arizona
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Jody B. Hice, Georgia
Glenn Grothman, Wisconsin
James Comer, Kentucky
Michael Cloud, Texas
Bob Gibbs, Ohio
Clay Higgins, Louisiana
Ralph Norman, South Carolina
Chip Roy, Texas
Carol D. Miller, West Virginia
Mark E. Green, Tennessee
Kelly Armstrong, North Dakota
W. Gregory Steube, Florida

DAVID RAPALLO, *Staff Director*
RICHARD TRUMKA, *Subcommittee Staff Director*
AMY STRATTON, *Clerk*
CONTACT NUMBER: 202-225-5051

CHRISTOPHER HIXON, *Minority Staff Director*

SUBCOMMITTEE ON ECONOMIC AND CONSUMER POLICY

Raja Krishnamoorthi, Illinois, *Chairman*

Mark DeSaulnier, California,
Katie Hill, California
Ro Khanna, California
Ayanna Pressley, Massachusetts
Rashida Tlaib, Michigan
Gerald E. Connolly, Virginia

Michael Cloud, Texas, *Ranking Minority Member*
Glenn Grothman, Wisconsin
Chip Roy, Texas
Carol D. Miller, West Virginia

C O N T E N T S

INDEX OF DOCUMENTS

IMPROVING DATA SECURITY AT CONSUMER REPORTING AGENCIES

Tuesday, March 26, 2019

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND REFORM,
SUBCOMMITTEE ON ECONOMIC AND CONSUMER POLICY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 3:40 p.m., 2154 Rayburn House Office Building, Hon. Raja Krishnamoorthi (chairman of the subcommittee) presiding.

Present: Representatives Krishnamoorthi, Hill, DeSaulnier, Pressley, Tlaib, Grothman, and Miller.

Mr. KRISHNAMOORTHI. The subcommittee will come to order. Without objection, the chair is authorized to declare a recess of the committee at any time. This hearing is entitled, Improving Data Security at Consumer Reporting Agencies. I welcome all of you here today. Thank you so much for coming. I now recognize myself for five minutes to give an opening statement.

The Subcommittee on Economic and Consumer Policy is dedicated to addressing the issues affecting American consumers and our larger economy. Today, we look at what can be done to improve data security by consumer reporting agencies, otherwise known as CRAs.

September 7, 2017, changed our data security landscape forever. That was the day that Equifax announced that it had exposed the social security numbers and other sensitive information of nearly half of all Americans. Specifically, 148 million Americans had their sensitive information exposed.

That event educated many people for the first time about CRAs and the huge amounts of sensitive information that they hold. What people still may not know is how many more of these companies exist in America. The Consumer Financial Protection Bureau, or CFPB, estimates that there are more than 400 CRAs today.

Criminals want access to the treasure troves of data that CRAs hold. They want that information so they can open fraudulent accounts and run up debt in the names of innocent people. In studying this issue, I was deeply saddened to learn about one Illinois resident whose credit was so badly damaged by identity theft resulting from the Equifax breach, that the person was denied both employment and housing.

This is but one example illustrating the extreme and decades-lasting implications of allowing peoples' social security numbers, birthdates, addresses, driver's license numbers, and credit card information to be exposed to cyber criminals.

Again, I want to let this sink in. This one particular breach, with regard to Equifax has the potential to cause extreme harm to nearly half of the population, or 148 million Americans.

A year and a half has passed since the Equifax breach and the causes of that breach have been investigated and exposed. Moving forward, it is our job in Congress to help prevent future data breaches and to prevent more Americans from having their sensitive, personal information compromised.

Through the Gramm-Leach-Bliley Act, otherwise known as GLBA, Congress directed the Federal Trade Commission to implement data security rules for CRAs. To achieve that, it created the, "Safeguards Rule," which requires CRAs to take, "reasonable steps to protect consumer data." But the FTC has limited recourse against the CRAs that violates the Safeguards Rule. It cannot seek penalties for first violations, and the FTC can only seek monetary compensation for consumers if they have identified a specific harm.

Because the negative effects of a breach can often take years to surface, it is extremely difficult to reduce this harm to a single dollar amount. CRAs also hold huge sway over the lives of consumers. The information they control could determine if someone gets a loan, a job, insurance, or a home. Yet, CRAs are not accountable to those same individuals.

If consumers dislike a CRA, they cannot hold them accountable by taking their business elsewhere. But Congress can and should hold CRAs accountable by giving Federal watchdogs the tools they need to make CRAs care more about data security.

Failure to implement proper data security must cost CRAs more than investing in good security to prevent a breach. That is why today, Senator Elizabeth Warren and Chairman Elijah Cummings released a proprietary report by the Government Accountability Office, the GAO, which we will closely examine in this hearing.

In this new report, GAO has recommended giving the FTC penalty authority for first violations to prevent breaches and to protect data security. This is a nonpartisan analysis, and in fact, democratic and republican FTC chairmen have called for increased penalty authority for first-time violations, including the current FTC Chairman, Mr. Joseph Simons.

Enhancing FTC penalty power to enforce data security follows the model set by regulations in the banking industry. There, so far, knock on wood, we have avoided the types of large, harmful data breaches that brought us here today.

Simply put, GAO does not think that the current regulatory system is strong enough to get CRAs to improve their data security. So far, many CRAs have been able to internalize the profit off of consumer data, externalize the risk, and leave consumers holding the bag.

Today's hearing is the first step in ensuring the data of American consumers is being properly protected. Now, with that, I would like to recognize our Distinguished Ranking Member, Mrs. Miller, sitting in for the ranking member. You have five minutes.

Mrs. MILLER. Thank you, Mr. Chairman. I do not have an opening statement, but I do want to thank you all, you witnesses, for appearing here today, and I look forward to your testimony and our discussion.

I also have the prepared remarks of Ranking Member Cloud, and I ask unanimous consent that they be inserted in the record.

Mr. KRISHNAMOORTHI. Without objection, so entered.

[The Prepared Statement referenced above follows.]

Committee on Oversight and Reform

Subcommittee on Economic and Consumer Policy

Ranking Member Michael Cloud Opening Statement

"Improving Data Security at Consumer Reporting Agencies"

Tuesday, March 26, 2019 at 2:00 p.m.

- Thank you, Mr. Chairman, and thank you everyone for being here for today's hearing on data security and credit reporting agencies.

- On September 7, 2017, Equifax announced a cybersecurity incident that affected 143 million consumers. This number eventually grew to 148 million—nearly half the U.S. population.

- It is not a stretch to say that this breach likely included the personal information of most people in the room today.

- Equifax in one of several large credit reporting agencies in the United States.

- These companies gather consumer data, analyze it to create detailed reports, and then sell the reports to third parties like financial institutions.

- Importantly, consumers do not usually provide information to these companies voluntarily.

- But if you have a credit card, mortgage, home equity loan, student loan, insurance, pay for utilities, rent property, or in some cases have applied for a job, these companies have information about you.

- Credit reporting agencies facilitate financial transactions by amassing large amounts of sensitive personal data on consumers and this makes them a high-value target for cyber criminals.

- These companies are subject to several federal laws designed to protect consumer information.

- These laws include the Federal Trade Commission Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and Dodd-Frank.

- These are primarily enforced by the Federal Trade Commission, who is represented on our panel today, and the Bureau of Consumer Financial Protection.

- Since the Equifax breach was announced, questions have been asked about whether these agencies have sufficient authority to ensure the security of consumer data.

- Congress must carefully weigh the advantages and disadvantages of providing new regulatory authority to a Federal agency.

- Any solutions must be based on specific, identifiable hams to consumers that are not adequately addressed by existing law.

- Congress should resist giving broad grants of power as a knee-jerk reaction to whatever is the crisis of the day.

- And we should be wary of creating top-down, one-size-fits-all regimes, as such solutions will have anti-competitive effects and will cement the role of incumbent players in the market.

- This is what we are seeing in Europe, with their recent implementation of the General Data Protection Regulation or GDPR.

- In the EU market, small internet advertising companies lost between 18 and 32 percent market share last year—while Google increased its online dominance.[1]

- While the GDPR seems to so far be succeeding in reducing the number of companies collecting online data from consumers, it is also succeeding in concentrating what data is collected with Google, Amazon, and Facebook.[2]

---

[1] Natasha Lomas, *GDPR Has Cut Ad Trackers in Europe But Helped Google, Study Suggests*, TECHCRUNCH (Oct. 9, 2018), https://techcrunch.com/2018/10/09/gdpr-has-cut-ad-trackers-in-europe-but-helped-google-study-suggests/.
[2] Mark Scott, Laurens Cerulus, and Laura Kayali, *Six Months In, Europe's Privacy Revolution Favors Google, Facebook*, POLITICO (Nov. 23, 2018), https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/.

- In the period before the GDPR came into effect, large companies set aside 6.8 billion Euros and hired thousands of lawyers to ensure their compliance.[3]

- Meanwhile, investment in European tech startups has fallen 40-percent from what it was before the GDPR was implemented.[4]

- If Congress wants to protect consumer choice, innovation, and small business, an expansive top-down regulatory regime is the wrong way to do it.

- In 1995, the most valuable tech company was NetScape.[5] You would be forgiven for not knowing what that is, because it doesn't exist anymore.

- What life-changing technology could we be depriving future generations if we institute a regulatory regime so expensive, complex, and onerous that only the biggest companies can afford to comply?

- I thank our witnesses for appearing before our subcommittee today and I look forward to their testimony.

- Mr. Chairman, I yield back.

---

[3] *Id.*
[4] *Id.*
[5] Eugene Kim, *It's Mind-Boggling How the 5 Most Valuable Internet Companies Have Changed Over the Past 20 Years*, BUS. INSIDER (Jun. 2, 2015), https://www.businessinsider.com/the-5-most-valuable-internet-companies-in-1995-vs-today-2015-6.

Mrs. MILLER. Thank you, Mr. Chairman, and I yield back.

Mr. KRISHNAMOORTHI. Thank you, Mrs. Miller. Today, we are joined by Mr. Andrew Smith, the Director of the Bureau of Consumer Protection of the Federal Trade Commission; Mr. Michael Clements, the Director of Financial Markets and Community Investment at the GAO; as well as Mike Litt, the Consumer Campaigns Director at U.S. Public Interest Research Group; and finally, Jennifer Huddleston, a Research Fellow at the Mercatus Center.

If the witnesses would please rise, I will begin by swearing you in.

[Witnesses sworn.]

Mr. KRISHNAMOORTHI. Let the record show that the witnesses answered in the affirmative. Thank you and please be seated. The microphones are sensitive, so please speak directly into them. Without objection, your written statements will be made part of the record.

I should tell you about the lighting system. I told a couple of you, but green means go; red means stop; yellow is different than what we see at stop lights. Here, you have to speed up, not slow down. So with that, why don't we begin with Director Clements? You are now recognized to give an oral presentation of your testimony.

STATEMENT OF MICHAEL CLEMENTS, DIRECTOR, FINANCIAL MARKETS AND COMMUNITY INVESTMENT, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CLEMENTS. Chairman Krishnamoorthi, Representative Miller, and members of the subcommittee, I am pleased to be here today to discuss a recent report addressing oversight of consumer reporting agencies or CRAs. Our bottom-line message: actions are needed to strengthen oversight at CRAs.

CRAs serve an essential function in the financial services industry. These companies collect large amounts of sensitive information about consumers. These companies maintain and analyze that information and ultimately package the information into consumer reports.

These reports help determine whether and how much consumers pay for credit and can also be used in employment and rental decisions among other purposes. At the same time, consumers have limited choice in the CRA marketplace. Unlike many other products and services, consumers cannot exercise choice if they are dissatisfied with a CRA.

Further, consumers do not have the legal right to delete their records with a CRA. CFPB and FTC have noted the level of consumer protection required can depend upon consumers exercising choice in the marketplace. Less choice implies the need for greater oversight.

The 2017 cyber attack on Equifax with the theft of at least 145 million consumers' records has focused attention on oversight of CRAs. With this context, a focus on FTC's and CFBP's oversight of data security in the CRA marketplace.

First, FTC. FTC enforces CRA compliance with the FTC Act and the Gramm-Leach-Bliley Act, or GLBA, among others. Section 5 of the FTC Act authorizes FTC to investigate and take enforcement

action against companies that engage in unfair or deceptive practices, including those related to data protection. FTC has taken action against 66 companies, including CRAs, under Section 5 for unfair or deceptive practices related to data protection.

GLBA seeks to ensure that financial institutions protect consumers' non-public information. As required by GLBA, FTC adopted its Safeguards Rules. Among other things, the Safeguards Rule requires that financial institutions assess the risk to consumer information and have a plan to mitigate those risks.

FTC can enforce the Safeguards Rule through injunction, redress, and discouragement. However, assessing monetary harm can be difficult with data breaches, because, for example, the resulting harm may occur years in the future. Thus, we recommend that Congress consider granting FTC civil money penalty authority for violations of GLBA. This would give FTC the tools to carry out the enforcement authority that Congress has already provided to FTC.

Second, CFPB. CFPB enforces and examines CRA compliance with several consumer protection laws, including the Dodd-Frank Act in portions of GLBA. Under the Dodged-Frank Act, CFPB supervises larger market participant CRAs. Those with more than $7 million in annual receipts from consumer reporting.

However, we found that CFPB does not have a good handle of the number of CRAs that meet its larger market participant threshold. Thus, we recommended that CFPB identify additional sources of information that would help ensure that it is tracking all CRAs that meet its threshold.

From 2015 through 2017, CFPB examined several CRAs. However, we found that its prioritizing process does not routinely account for data security risk. To determine specific areas of compliance to assess, CFPB considers sources such as consumer complaints and past exam finding. While important, these sources do not consider how an institution would detect and respond to cyber threats.

Following the Equifax cyber attack, CFPB initiated data security exams of the major CRAs, but it is unclear whether and how CFPB would incorporate data securities into its prioritization process going forward.

Thus, we recommended that CFPB assess whether its process for prioritizing CRA examinations sufficiently incorporates data security risks that CRAs pose to consumers' information.

Chairman, Krishnamoorthi, Ranking Member Miller, and members of the subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have.

Mr. KRISHNAMOORTHI. Thank you very much, Mr. Clements.

Mr. Smith, please.

STATEMENT OF ANDREW SMITH, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. SMITH. Thank you, Chairman Krishnamoorthi. Mr. Chairman and members of the subcommittee, I am Andrew Smith. I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission. I appreciate the opportunity to appear before you here today to discuss data security at the consumer reporting agencies.

I also want to thank Mr. Clements and GAO for its recently issued recommendations to improve the tools available to the FTC to enforce the data security laws applicable to consumer reporting agencies.

My written statement represents the views of the commission. This opening statement represents my ideas alone and not necessarily the views of the commission or any individual commissioner.

To promote the security of consumers' personal information, including information at the credit bureaus, the FTC focuses on three main areas. The first of these is enforcement. For nearly two decades, the FTC has been the Nation's leading data security enforcement agency, where charged with enforcing data security requirements contained in specific laws, such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. We also enforce Section 5 of the FTC Act, which prohibits unfair or deceptive practices, including unfair or deceptive practices with respect to data security.

In this law enforcement role, the commission has settled or litigated more than 60 actions against businesses that allegedly failed to take reasonable precautions to protect consumers' personal information. In 2017, the commission took the unusual step of publicly confirming its investigation of Equifax and the Equifax data breach, due to the scale of public interest in the matter.

Our second area of focus is policymaking. The FTC has conducted workshops, issued reports, and made rules to promote data security. For example, just earlier this month, we announced a notice of proposed rulemaking to update our Safeguards Rule under the Gramm-Leach-Bliley Act.

The Safeguards Rule was originally issued in 2002. It requires financial institutions within the FTC's jurisdiction, including credit bureaus, to implement reasonable process-based safeguards to protect personal information.

The proposed revisions to the Safeguards Rule are based on our nearly 20 years of enforcement experience. These revisions are intended to retain the process-based approach of the Safeguards Rule and to provide financial institutions with more certainty regarding the FTC's expectations with respect to data security.

Our third area of focus is education. The commission has issued numerous guidance documents for businesses including written materials, blog posts, and a comprehensive small business cyber education campaign, which includes, how-to videos and training materials. These materials distill lessons learned from our enforcement actions in a succinct and accessible manner.

With respect to cyber security at credit bureaus, the education of consumers is also critically important. Following the Equifax breach in September 2017, we established a dedicated web page for victims of the breach. During that first month, the FTC blog on the Equifax breach reached the most viewed Government webpage, nationwide, surpassing pages for disaster assistance after major hurricanes. The FTC's Credit Freeze FAQs article and IdentityTheft.gov recovery steps also made the top five most viewed Government webpages in September 2017.

We vigorously use our existing authority to protect consumers, but we need additional tools. In this regard, we appreciate and

agree with GAO's recommendation to give the FTC civil penalty authority for violations of the Safeguards Rule.

In fact, however, we have called more broadly on Congress to enact comprehensive data security legislation that includes rulemaking, civil penalty authority, and enhanced jurisdiction for the FTC.

First, the legislation should authorize the FTC to issue data security rules under the Administrative Procedures Act, so that we can keep up with business and technological changes. Where we currently have rulemaking authority, we have used it, as demonstrated by the proposed revisions to the Safeguards Rule, which I just mentioned.

Second, the legislation should allow the FTC to obtain civil penalties for data security violations. Currently, we have authority to seek civil penalties for data security violations under the Children's Online Privacy Protection Act and the Fair Credit Reporting Act, and we have used it. To help ensure effective deterrents, we urge Congress to enact legislation to allow the FTC to seek civil penalties for data security violations in appropriate circumstances.

Now finally, the legislation should extend the FTC's jurisdiction over data security to nonprofits and common carriers. Entities in these sectors often collect sensitive consumer information and significant breaches have been reported, particularly in the nonprofit educational and hospital sectors.

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

Mr. KRISHNAMOORTHI. Thank you, Mr. Smith.

Mr. Litt, you have five minutes.

STATEMENT OF MIKE LITT, CONSUMER CAMPAIGNS DIRECTOR, U.S. PIRG

Mr. LITT. I am sorry about that.

Mr. KRISHNAMOORTHI. Take two.

Mr. LITT. All right, good afternoon. Again, my name is Mike Litt with U.S. PIRG. I appreciate the opportunity to testify before you today.

In order to improve data security at credit reporting agencies, also known as credit bureaus, we need robust financial penalties, stronger oversight, and better consumer control of our data. You mentioned the Equifax breach. All we have to do is look at that to see the real dangers that are posed to real people when credit reporting agencies drop the ball on their data security and lose our data.

I am one of the 148 million Americans whose financial DNA was exposed, and we are put at risk of identity theft and all sorts of fraud for the rest of our lives. Equifax still has not paid a penalty after putting people in harm's way. We have no choice over Equifax or the other credit bureaus—that can collect our information and sell it.

And when they lose it, we cannot leave them the way we can other companies. It is exactly that dynamic, why it is important that we have robust financial penalties when data is lost and strong oversight to prevent data loss in the first place.

If you are a larger credit bureau and you do not comply with the Federal Trade Commission's Safeguards Rule. There should be mandatory penalties. If you lose personal data, there should be mandatory fines, but at the very least, we need to make sure that the FTC can actually issue penalties for the first violation of the law. They investigated the Equifax breach, but they will only be able to issue a consent order and then only if Equifax breaks that order and then violates the law a second time can there actually be any fines. We need to change that.

Next, I would like to discuss some ideas for oversight from my written testimony. The Consumer Financial Protection Bureau does have tools that the FTC does not. It can issue civil penalties after first violation of the law. It can examine companies to catch problems ahead of time.

We know from Equifax's SEC filing last month, that the CFPB has been investigating the Equifax breach, and they have expressed their intent to actually issue civil penalties.

So clearly, the CFPB is using its authority to take action on data security. We would like to see them consider and prioritize data security for examinations of other companies as well. The oversight committee's report on the Equifax breach that came out in December shows that hackers exploited unencrypted info and weak data controls. The FTC just proposed an amendment to its Safeguards Rule that would require some good first steps for security measures, such as data encryption and multi-factor authentication and data controls.

Finally, I would like to talk about better consumer control over our own data. The best way to stop an identity thief from opening new accounts in your name is to get credit freezes, also known as security freezes at all three of the national credit bureaus. Basically, a credit freeze blocks or freezes access to your credit reports.

Before the Equifax breach, the credit bureaus charged fees for freezes in most of the states. After the breach, 19 states made freezes free. Congress followed suit. Passed a law that eliminated fees for everybody. In my written testimony, I explain problems with the national freeze that we would like to see fixed, and we have got some other ideas in there for better consumer control.

But really the best solution would be to make sure that access to our own credit reports is actually frozen automatically by default. We should not have to opt in to control access to our own data.

So to summarize all of this, we are not the customers of the credit bureaus, but the credit reporting agencies possess vast amounts of our personal information, including our financial DNA and that is really why we need to be able to have robust financial penalties and stronger oversight to incentivize them to protect our data.

The FTC and the CFPB should use their authorities and be granted expanded authorities in order to achieve those goals. Additionally, we should be given more control over our own personal data.

I look forward to working with you. Thank you so much.

Mr. KRISHNAMOORTHI. Thank you, Mr. Litt.

Ms. Huddleston, you have five minutes.

STATEMENT OF JENNIFER HUDDLESTON, RESEARCH FELLOW, MERCATUS CENTER AT GEORGE MASON UNIVERSITY

Ms. HUDDLESTON. Thank you. Good afternoon. Chairman Krishnamoorthi, Representative Miller, and distinguished members of the Economic and Consumer Policy Subcommittee.

My name is Jennifer Huddleston, and I am a Research Fellow with the Mercatus Center at George Mason University. My research focuses, primarily, on the intersection of law and technology, including the important issue surrounding data security and data privacy.

Thank you for the opportunity to discuss some of these issues today, particularly in regards to the 2017 Equifax breach. These conversations are particularly important as we continue to see headlines around data breaches and data privacy.

As policymakers consider how to address such concerns, they should be careful to avoid unintended consequences to innovation, as a result. With this in mind, I would like to focus on three key points today.

First, that regulators should avoid an overly expansive definition of harm in their approach to data security to avoid unintended consequences to innovation. Second, the way the FTC's current enforcement approach has provided a balanced approach to data security and data privacy allowing innovation to flourish and providing consumers a form of redress. Finally, with regards to credit reporting agencies, that policy solutions should be narrowly tailored and focused on the unique position of these agencies and the data they possess, so as to avoid, or limit, unintended consequences to broader data base industries.

To begin, regulators should be cautions about an overly expansive definition of harm and their approach to data security that could have unintended consequences to innovation. While there is general agreement that data breaches have the potential for harm, there is disagreement on when harm occurs, the need for Government intervention, and what particularly constitutes harm in these scenarios.

There is a wide range of personal preferences and what information we choose to share publicly or privately through various data systems. A flexible system provides options for both consumers and businesses and encourages innovative solutions when it comes to data security. While it is easy to rush to the worst conclusions when we see scary headlines and hear news of breaches such as Equifax, only focusing on the bad could prevent future innovation that would provide better alternatives and better data security, more generally.

A lack of flexibility and a rigid system could lock in existing options, rather than providing incentives to innovate and provide better data security, more generally.

Now I would like to turn to the general success of the FTC's current enforcement approach with regards to balancing innovation and redress for consumer harm. The FTC has been active in both personal data and credit reporting and financial privacy. It has addressed data breaches under both deception and unfairness doctrines as well as other laws when specified.

But in general, it has built a common law of consent decrees, rather than more formal regulation and adjudication. While this allows for greater flexibility as innovation evolves, it also can raise concerns due to lack of clarity and certainty for regulated parties.

At the same time, though, this approach has allowed consumers benefits of a data-driven economy while still providing redress when consumer harm occurs.

Finally, with regards to the unique situation of credit reporting agencies, the policy solutions in regard should be narrowly tailored so as to avoid unintended consequences to data base industries, more generally.

The credit reporting agencies are in a unique situation, in that there is no opt in or opt out for consumers. Additionally, due to high barriers to entry, there may be less concern about potential impact on competition that such regulation could have.

Given these factors, the policy solutions to address these concerns with regards to data breaches and data security should focus on these unique aspects and the data that is uniquely concerning when it comes to these agencies.

At the same time, though, we should also consider, what, in addition to regulation, or as an alternative to regulation, might be done more generally. For example, consumer education and empowerment, including increased transparency so that consumers are aware of what to do in the event of data breaches and what resources are available to them. As well as common law alternatives for those that have experienced harm and accountability for those who caused it.

The U.S. has been a leader in innovation, and this makes it especially important to carefully consider the potential for unintended consequences and not prevent potentially innovative solutions that would provide better security in the future.

Thank you, and I welcome your questions.

Mr. KRISHNAMOORTHI. Thank you, Ms. Huddleston.

First of all, thank you to all of you for joining us today. All of the witnesses, and of course, the members of the audience.

I want to start with Mr. Litt. I recognize myself for five minutes of questions.

You know, Equifax had very sensitive information about at least 148 million people: their names, social security numbers, addresses, dates of birth and so on. Do the other CRAs have similar information about as many consumers?

Mr. LITT. Yes, in fact it is probably more. The CFPB has said that each of the credit bureaus possess approximately 200 million different consumer files.

Mr. KRISHNAMOORTHI. I mentioned some types of personal information. Are there other types of sensitive information they possess?

Mr. LITT. Well they have information that is in our credit files that could show whether you are in debt or debt collection, your credit history. Also credit bureaus have investigative reports on some consumers. So these are basically background checks that can include interviews with your coworkers, your neighbors, your friends and family, other people in your life.

Mr. KRISHNAMOORTHI. Do you have any indication that CRAs are collecting less information today than they were at the time of the Equifax breach?

Mr. LITT. No, I have absolutely no indication of that.

Mr. KRISHNAMOORTHI. Can you explain a couple of the more serious risks that consumers face when their sensitive data is exposed?

Mr. LITT. Yes, so in the case of the Equifax breach where you have just your name and your social security number, an identity thief can try to apply for a utilities account, credit, a loan, get a smart phone on your account. Then they can use your date of birth and they can try to apply for your social security benefits, your tax refund that you might be counting on, your medical services and benefits.

Mr. KRISHNAMOORTHI. Okay, without objection, I would like to enter into the record, a complaint submitted to the Consumer Financial Protection Bureau by an Illinois parent who was a victim of the Equifax data breach.

Mr. KRISHNAMOORTHI. This was the complaint and, you know, I read a portion of this earlier, or read about it earlier. But basically, this person was unable to receive housing or employment because of the harm from the data breach.

Director Smith, I have a question for you. With their high concentration of sensitive information, are CRAs subject to constant attack by cyber criminals? What is the nature of the attacks and the threats posed by cyber criminals?

Mr. SMITH. So that is probably a better question for the credit bureaus, but, you know, our understanding is that financial institutions, generally, and credit bureaus, specifically, are subject to constant attack, given the value of the information that they warehouse.

I think what you find is if you spoke with financial institutions, they would say that they are under constant attack. That is one of the issues for us in the FTC. We want to make sure that financial institutions are always monitoring for penetration and intrusion so that the breaches are actually being detected. Because that is one of my real fears — that there are breaches that are going undetected.

Mr. KRISHNAMOORTHI. Well that is what I was going to ask you next. Equifax may have garnered the most attention, but, you know, can you talk about other data breaches at any other CRAs in recent years?

Mr. SMITH. Well we have brought some enforcement actions in connection with data breaches at consumer reporting agencies. The most prominent is probably our action against ChoicePoint several years ago where they were selling credit reports to a ring of known identity thieves. There we sought—well we obtained $10 million in penalties and $5 million in consumer redress.

I will say that most of the cases of the 66 cases that Mr. Clements mentioned in the data security area, a couple have involved credit bureaus but mostly not. It is mostly other types of companies and primarily operating online.

Mr. KRISHNAMOORTHI. Got it. Mr. Clements, can I ask you the next question? Can you identify other, you know, regulatory areas where, you know, the penalty for a first violation has been found

to be effective or, you know, what's the nature of the impact of such a type of penalty?

Mr. CLEMENTS. We do know in the banking space that the Federal banking regulators, that would be, for example, Office of Comptroller of the Currency, the Federal Reserve, and FDIC, do have civil penalty authority under GLBA for those type of violations.

They are also examining these institutions on a regular basis. If it is a larger institution, it is subject to continuous reviews. If it would be a smaller institution, every 12 to 18 months there would be an examination.

Mr. KRISHNAMOORTHI. Got it. I am out of time. I am going to recognize Mrs. Miller for the next set of questions.

Mrs. MILLER. Thank you, Mr. Chairman.

Ms. Huddleston, in your testimony you state that the Federal Trade Commission's current approach has been flexible and therefore has allowed innovation to flourish while still protecting consumers. Can you please expand upon that?

Ms. HUDDLESTON. Thank you, Mrs. Miller. I would point to the fact that the Federal Trade Commission has been active in data breaches and data privacy going back to the late 1990's with GeoCities. Our data security and our innovation when it comes to online websites and what we expect them to protect has come a long way. Part of this has been rather than having an ex-ante approach of regulation, they have been able to provide a flexible guidance that allows different methods to develop to better protect consumers.

Mrs. MILLER. Thank you. While it may sometimes be a useful tool, enforcement actions by Federal agencies should not be the only way to ensure consumer data is safe. Would you agree?

Ms. HUDDLESTON. One of the interesting elements with enforcement actions is how once they are enacted they can be unflexible and unmoving. This can affect both consumers and companies that are subject to consent decrees. At the same time, there are also already existing tools, including the common law for consumers who may have direct proof for harm of something like identity theft. There can also be criminal issues involved depending on the nature of what has happened as a result of the breach.

Mrs. MILLER. What are the pitfalls of excessive Government intervention in a rapidly evolving area like information technology?

Ms. HUDDLESTON. We have benefited a lot from innovation and many of us have seen how rapidly, in our lifetime, things have changed as a result of allowing innovation to accelerate. If we have a lot of regulation in a rapidly changing area, such as data security, it is possible we may lock in the existing system, rather than getting a better system that could protect our data more.

Mrs. MILLER. What are some buffers that could be created to narrowly tailor regulatory authority?

Ms. HUDDLESTON. When considering what to do with regards to the credit reporting agencies, such as Equifax and these concerns, I would suggest that we look very carefully at how we are defining data and how are defining what entities are covered. So that we are truly addressing those concerns.

Mrs. MILLER. What can the Federal Trade Commission do to provide greater education to consumers?

Ms. HUDDLESTON. I think that in light of the Equifax breach, what we have seen is a lot of consumers really want to get interested in how they can protect themselves and take those steps as we heard mentioned in earlier testimony.

Immediately after the Equifax breach, the blog post on what to do was one of the most visited Government websites. Continue to provide that information to consumers, be it through websites or through other educational campaigns, so that consumers can then take the appropriate and next steps themselves.

Mrs. MILLER. Thank you. We have heard a lot recently about the General Data Privacy Regulations, or GDPR, in Europe and the California Consumer Privacy Act, or CCPA. What are the problems with expansive, top-down regulatory regimes such as this?

Ms. HUDDLESTON. With the GDPR, we have already seen that there are fewer data actors in Europe. You already had a very top-down regulatory regime, but smaller players have had to exit the market, in some cases, because of the cost of compliance.

Therefore, you may not be getting innovative solutions that could be more protective, and you are not seeing the type of competition that we would like to see when it comes to that, that can provide better security.

Mrs. MILLER. Thank you. Mr. Chairman, I have here three letters addressed to our subcommittee concerning issues before us today. The first is from the R Street Institute, a nonpartisan think tank. The second is from the National Association of Federally Insured Credit Unions. And the third is from the Credit Union National Association. I ask unanimous consent that these letters be inserted in the record.

Mr. KRISHNAMOORTHI. Without objection, so entered.

Mrs. MILLER. Thank you. I yield back my time.

Mr. KRISHNAMOORTHI. Thank you, Mrs. Miller.

Ms. Pressley, you are on the clock for five minutes.

Ms. PRESSLEY. Thank you, Mr. Chair, and I want to thank all of our witnesses for joining us today. It is clear from your testimony that consumer reporting agencies occupy a very unique space.

They deal in consumer data, but they do not deal with consumers. Their customers are businesses. Their products are the data that they gather about you and me and millions of other Americans. They have the power to affect peoples' lives in critical ways. They provide the reports that determine everything, from whether you can get a loan to whether you can obtain housing or even employment. Yet, they put people at risk when they lack adequate data protection safeguards like we saw with the Equifax breach which impacted nearly 148 million consumers in 2017.

In fact, last month at a hearing held by the Financial Services Committee, which I am a member of, I asked the CEO of Equifax whether anyone on their leadership team was held accountable for this data breach. His response was, "There was plenty of accountability. The entire leadership team in 2017 did not receive a bonus."

This is, I am sure, you would agree, an insult to the millions of consumers that were affected by the breach and continue to this

day to struggle to bounce back after having their data compromised.

So I want to touch on what options, if at all, consumers have in this market. You spoke to some of this you—all of you—in your testimony. If you could elaborate, where clearly there is no accountability for CRAs when breaches like this happen.

Director Clements, in the GAO report you explain that consumers lack choices in the consumer reporting market. So if we could unpack that, just for the record, "Consumers are not voluntarily providing their data to CRAs. Business are not voluntarily providing their data to CRAs." Businesses are doing that, correct?

Mr. CLEMENTS. Consumer data ultimately is input to the process. So you are correct.

Ms. PRESSLEY. Okay. So, consumers are never actively providing consent for our data to be provided to CRAs. Again given your testimony, that is an accurate characterization, correct?

Mr. CLEMENTS. Right.

Ms. PRESSLEY. Okay. So if a constituent of mine is dissatisfied with Equifax's data protection practices, can he or she choose to remove their data to the competitor's and only have Experian and TransUnion maintain their files?

Mr. CLEMENTS. No.

Ms. PRESSLEY. Well what about leaving the consumer reporting market, entirely? Could someone force the CRAs to delete their records?

Mr. CLEMENTS. The CFPB has told us that consumers have no legal right to remove their data from a CRA.

Ms. PRESSLEY. Okay and so consumers do not voluntarily opt in to have their information shared to the CRAs, nor can they opt out? Instead, businesses are providing it, whether consumers want them to or not. And once the CRAs have the information, consumers are essentially locked out, correct?

Mr. CLEMENTS. That is correct.

Ms. PRESSLEY. Okay. Mr. Litt, I have a couple of minutes left. Most other private businesses cannot avoid consumers the way CRAs can. Most businesses have to try to consumers happy or risk losing them to their competitors. But CRAs are different. Can consumers make decisions with their dollars that would incentivize CRAs to ensure that they protect the sensitive data about their customers?

Mr. LITT. No, they have no say in the matter.

Ms. PRESSLEY. Without the pressure of market forces, is data security at CRAs a necessary area for Government regulation?

Mr. LITT. Absolutely.

Ms. PRESSLEY. Back to you, Director Clements. The GAO report indicates that CFPB has identified credit reporting as a higher risk market for consumer harm. Can you explain why it made that determination?

Mr. CLEMENTS. I cannot explain CFPB's logic. Our logic, what we think CRA is a high-risk area. One is it serves an essential function in the marketplace, in financial services industry. Second would be the large amount of sensitive information that is contained there. Then third, the fact that consumers have limited choice in this marketplace.

Ms. PRESSLEY. Thank you. So without consumer choice, CRAs lack the same market pressures as typical businesses to adequately protect consumer data. That is a market failure, and it reinforces the need for strong Government rules to help ensure sufficient consumer data protection at CRAs.

Thank you all for your testimony here today, your expert testimony. I look forward to working with all of my colleagues so that we can provide ample oversight and accountability for these CRAs, since clearly, they cannot be trusted to do that themselves.

Thank you. I yield my time.

Mr. KRISHNAMOORTHI. Thank you, Ms. Pressley.

Now, Mr. Grothman. You have five minutes.

Mr. GROTHMAN. Very good. I will start out with a question for Mr. Smith. Am I correct in saying that the FTC has authority to take enforcement action against credit reporting agencies that do not properly protect consumers' personal identifiable information or that act in an unfair and deceptive manner when it comes to consumers' personal data?

Mr. SMITH. Yes. We enforce the Fair Credit Reporting Act against consumer reporting agencies. We enforce our Safeguards Rule against consumer reporting agencies. As you noted, we have general authority to prohibit unfair and deceptive practices.

Mr. GROTHMAN. You brought over 60 cases against companies since 2002?

Mr. SMITH. For data security violations, yes.

Mr. GROTHMAN. You brought 30 cases against companies for violating the Gramm-Leach-Bliley Act, including the Safeguards Rule?

Mr. SMITH. That sounds Okay to me. That sounds right.

Mr. GROTHMAN. What is the process for bringing one of these cases?

Mr. SMITH. Generally we would learn of the case through a variety of means. It might be press reports. It might be consumer complaints. It might be tips or reports from other agencies. Then we will usually issue a civil investigative demand, which is an administrative subpoena to the company and conduct the investigation through the normal course.

Mr. GROTHMAN. As a practical matter, my data has been breached, how do I find out about it?

Mr. SMITH. You will generally find out about it because the company notifies you, because there are, in every state, there are laws that require companies where there is an authorized access or acquisition of data, requires the company that has been breached to send the affected consumers a notice.

Mr. GROTHMAN. Okay, but as a practical matter, that is if the company identifies or contacts me themselves. What bad thing would happen to me that I would find out about it? Or how often, when there is a breach, do bad things happen?

Mr. SMITH. So it is very difficult for us to say how often, when there is a breach, do bad things happen. Every once in a while, we can actually tie breached information to subsequent fraud against consumers. One example of that is when there was, I think it was the Yahoo had their user names and passwords that consumers used at other sites. So, there was a sum ability to link, but gen-

erally, the proximate causation of compromised data to any eventual consumer harm, that can be a difficult thing to show.

Mr. GROTHMAN. Okay. How many people, do you think, had bad things happen because of this? Do you have any idea?

Mr. SMITH. Because of?

Mr. GROTHMAN. Of the breaches.

Mr. SMITH. Of breaches generally or of the Equifax breach, specially?

Mr. GROTHMAN. Well, both.

Mr. SMITH. So we spend a lot of time studying identity theft in the economy, generally. We know that there is sort of a background level of identity theft. In any given year, a certain number of us will be subject to identity fraud. The reasons for that may be difficult to discern.

What we are looking at when we try to look at sort of gross aggregate levels of harm to consumers is following a big breach like Equifax, is there any change to that background level of identity theft?

My understanding, and again, I am not commenting on any particular investigation that we have in front of us. But my understanding is that Equifax has claimed that there has not been any increase, generally, in the gross level, of identity theft. But that just could mean that the information has not yet been used.

Mr. GROTHMAN. Okay. Do we have any hard numbers as far as in the Equifax breach? How many people had a bad thing happen to them? Not getting a letter in the mail saying that, you know, your identity has been breached, but a bad thing was done with that information?

Mr. SMITH. Right. I think that is going to be very difficult for anyone to show. I mean, the bad things that we would be thinking about would be someone opening a credit card in your name, for example. That is the causation, the cause of link between the Equifax breach and that new account opening in your name.

Mr. GROTHMAN. They really do not know. Nobody knows. Okay.

Ms. Huddleston, you are a scholar focusing at the intersection of technology and the law. Do you think the FTC has an approach to ensuring data privacy and security has been effective so far?

Ms. HUDDLESTON. The good thing about the FTC's approach to data privacy and security is that it has been flexible to move with the technology. The concern is that, because it is often done through consent decrees, it does not necessarily provide regulated entities with the knowledge of what is constantly expected of them. At the same time, our court system and the common law may be able to provide redress for those consumers who do have the measurable harm you were mentioning in your earlier question.

Mr. GROTHMAN. Okay. I think I have time for one more question. This is kind of a little bit off the topic, but just in general, I always think with these agencies, the major concern is that there are flaws in their information, in which you could be harmed, and you do not even know that you are being harmed.

Do you think we are doing an adequate job of policing that potential problem? In other words, if there are Glenn Grothmans in the world, and the other guy is a spendthrift, to what degree are we

catching that sort of thing? Or to what degree are people's credit score being harmed unfairly? Do we catch that sort of thing?

Mr. SMITH. So I can start on that. I think that mistaken identity is a big problem in the credit reporting system. We want to make sure—so my name is Andrew Smith. There are tens of thousands of Andrew Smiths. How do I make sure that a bad Andrew Smith does not get mixed up with me? Or how do I make sure that his information does not wind up in my file? Those are challenging issues that are a part of the data security issues, right, but they do not have to do with data quality.

Mr. GROTHMAN. Right. It is not exactly on point, but I think probably insofar as you worry about these agencies. I guess with what we have done, we will go one. The chairman is giving me the hook. That is Okay.

Mr. SMITH. Well I will say that we brought a case, just a couple of months ago, for this very accuracy issue, where there was information about a bad person showing up in your file. It was against a company called Real Page and we obtained a $3 million penalty under the Fair Credit Reporting Act. So there are laws against it, and they are enforced.

Mr. GROTHMAN. Thank you.

Mr. KRISHNAMOORTHI. Very good. Thank you.

Ms. Tlaib, you have five minutes.

Ms. TLAIB. Thank you. I want to thank all of our witnesses today for joining us. Director Clements, I would like to discuss the Consumer Financial Protection Bureau's role in ensuring data security at consumer reporting agencies. In Michigan alone, close to 4.6 million consumers were impacted by Equifax's unprecedented data breach.

My constituents, of course, do not have the luxury of constant credit monitoring. So it is imperative that we remain diligent in our oversight of these credit reporting agencies, especially now that they are using credit scoring and reports for car insurance and other elements directly impacting people's quality of life.

How many CRAs fall within CFPP's larger participant supervisor power?

Mr. CLEMENTS. CFPB has told us it is tracking between 10 and 15 of those companies.

Ms. TLAIB. The GAO report, the Government Accountability Office report recommends that CFPB leverage traditional resources of information to make sure it is tracking all CRAs that may qualify, why?

Mr. CLEMENTS. CFPB told us that it was unsure whether that was the exact number of companies that its threshold of $7 million of annual receipts. So there could be a few additional companies.

Ms. TLAIB. Has CFPB indicated a willingness to do that?

Mr. CLEMENTS. CFPB has mentioned a willingness to leverage other data sources.

Ms. TLAIB. To fulfill its mission, it is important the CFPB knows all of the CRAs that falls within its jurisdiction. So the CFPB has the power to conduct supervisor examinations of CRAs. After the Equifax breach, the GAO report indicated that CFPB even developed internal guidelines for examining data security. Did CFPB actually conduct any examinations of data security at CRAs?

Mr. CLEMENTS. Our understanding is that following the Equifax breach, the CFPB has conducted multiple targeted data security exams at CRAs. What it was not doing was incorporating that type of information prior to the Equifax breach. So it was not looking at data security prior to the breach.

Ms. TLAIB. The GAO report indicated that CFPB has the authority to conduct these data security examinations of CRAs—these acronyms in D.C. I cannot believe it. Pursuant to its general authority to assess compliance with Federal consumer protection laws, such as Dodd-Frank Act, preventing any fair, deceptive, and abusive acts in practice. Yet, The GAO report indicated that CFPB has not committed to continue considering data security risks in selecting examinations going forward. Is that correct?

Mr. CLEMENTS. That is correct.

Ms. TLAIB. GAO's report also said, in light of the Equifax breach, as well as the CFPB's acknowledgement of the CRA market as a higher risk market for consumers, it is important for CFPB to routinely consider factors that could inform the extent that CRA data security risks, such as the number of consumers that could be affected by a data security incident and nature of potential harm, resulting from the loss of exposure of information.

So this GAO report recommends continue[ing] to prioritize the risk of data breach in selecting examination topics. Can you explain why that is particularly important?

Mr. CLEMENTS. Certainly. In the past, what CFPB was looking at when it was doing the supervision was focusing on consumer complaints, past exam filings and public filings. So they ended up looking at issues such as the accuracy of the data and the dispute resolution process. We do not dispute at all that those are important, but it was not factoring in the risk to consumer information that a breach might happen.

That was...just within the prioritization process. Does that mean that in every instance they would need to do that type of exam? At least you are considering it when you are making a decision of, ″I am going to do an exam of a CRA. What factors should I look at in that assessment?″

Ms. TLAIB. Thank you. The report also noted that other institutions that hold sensitive consumer data like insured depository institutions are already subject to technology examinations, which include cyber security component. Would we not want the same kind of supervision on CRAs as we have for banks?

Mr. CLEMENTS. I think our findings really get to two points. On the one hand is factoring in on those examinations that CFPB is conducting data security. Then the other recommendation we make in D.C. is to have some predictability and a penalty available should the firm not meet the requirements in that case of Gramm-Leach-Bliley. So really, our findings were a combination of both examinations and the penalty.

Ms. TLAIB. Okay, thank you so much. I yield my time.

Mr. KRISHNAMOORTHI. Thank you, Ms. Tlaib.

Ms. Hill, you are up for five minutes.

Ms. HILL. Thank you, Mr. Chairman and thank you all for being here. I know you have touched on the answers to some of these,

but I want to get clarification on a few things and just get this for the record.

Director Clements, I would like your help in understanding the scope of the credit reporting market. People may be familiar with the big three: Equifax, Experian, and TransUnion, but I was struck by the following statement in the GAO report, which states, "According to the CFPB, the consumer reporting market comprises more than 400 companies, and these companies issue three billion reports and make more than 36 billion updates to consumer files each year."

So beyond the big three, there are hundreds of these companies out there, each holding our sensitive information. Is that correct?

Mr. CLEMENTS. That is our understanding from CFPB, yes.

Ms. HILL. Great. These CRAs have subsidiaries that conduct marketing activities. The GAO report indicates that CRAs are able to share information with their affiliates for marketing purposes as long as they disclose that and give consumers an option to opt out. Is that right?

Mr. CLEMENTS. It depends on the relationship that the individual would have with the credit reporting agency. If I have a relationship with the credit reporting agency, for example, if I am buying a credit monitoring service, the credit reporting agency can then share that information with its other affiliates. But again, it needs to provide notice, opt out option. Then I, as the consumer, would have to not opt out. If that is the case, there can be sharing with other affiliates within the CRA.

Ms. HILL. What would another case be where they would not have the sharing opportunity?

Mr. CLEMENTS. If I am not a customer of the CRA, then I do not have a customer relationship and then the rules are slightly different.

Ms. HILL. Different how?

Mr. CLEMENTS. There would be less sharing opportunities in that case, because again, I am not a customer in that instance.

Ms. HILL. Okay. So in addition to consumers being concerned about their information being breached through the backdoor, they also have to worry about it leaving through the front door on its way to the marketing arms of the CRA. Is that right?

Mr. CLEMENTS. Again, it depends on the customer relationship and whether the customer choose the opt in or opt out of the sharing.

Ms. HILL. I mean, actually like it is not usually, even you "opt in or opt out" it is not a very transparent process. I think it is usually you check a box, because you are trying to hurriedly fill out a form to get something that you need, but is that what you are referring to?

Mr. CLEMENTS. I think in terms that the specifics we did not get into that. I probably defer to FTC or CFPB in terms of the ease of a customer opting in or opting out.

Ms. HILL. Okay. Director Smith, FTC published a helpful guidance to companies about complying with the Safeguards Rule that you make available online. It is entitled, "Financial Institution and Customer Information: Complying with the Safeguards Rule." In the How to Comply Section, it states, "One of the earliest steps

companies should take is to determine what information they are collecting and storing and whether they have the business need to do so. You can reduce the risks to customer information if you know what you have and keep only what you need."

Director Smith, it does not appear that CRAs were heeding that advice prior to the Equifax breach. Since then, have you seen any indication that CRAs have downsized the amount of data they are keeping about us?

Mr. SMITH. So we do not have any information about them downsizing the information. I would say that, that guidance is more sort of directed at companies being mindful of the information that they have, inventorying it, and making sure that they still have a need for it. I suspect that if we were to ask the CRAs, they would say, "This is information that we need."

Ms. HILL. Okay. Do know if Equifax or any of the other CRAs have reduced their use of social security numbers?

Mr. SMITH. Not to my knowledge, no.

Ms. HILL. Okay, Mr. Litt, social security numbers are used both as identifiers and authenticators, can you please explain the difference?

Mr. LITT. Sure an identifier basically matches your file, matches you to your file. And an authenticator proves who you say you are. So you can think of an identifier as a username and an authenticator as a password.

Ms. HILL. Okay so, in theory, an authenticator should be something secret that only you can provide. Is that right?

Mr. LITT. That is right.

Ms. HILL. So after Equifax exposed so many social security numbers, they are no longer a secret, should CRAs stop using them as authenticators?

Mr. LITT. Yes, they should start using them, at least as part of their authentication process.

Ms. HILL. Does the continued use of social security numbers as authenticators help fuel identity theft?

Mr. LITT. Yes, they do, especially with the Equifax breach, because that is more than half the adult population, and you cannot change them.

Ms. HILL. Do you know if Equifax or the other CRAs have stopped using social security numbers in the authentication process?

Mr. LITT. I am not aware of that.

Ms. HILL. So at this point, social security numbers are widely known, and I would like to see companies acting accordingly and to stop using them as authenticators. Thank you so much.

Mr. KRISHNAMOORTHI. Thank you, Ms. Hill.

With unanimous consent, I enter the following statements into the record. I have a letter from the Conference of State Bank Supervisors and a letter from the Electronic Privacy Information Center.

Without objection, so entered.

Mr. KRISHNAMOORTHI. I would like to thank our witnesses for their testimony today. Without objection, all members will have five legislative days, within which, to submit additional written questions for the witnesses, to the chair, which will be forwarded

to the witnesses for their responses. I ask our witnesses to please respond as promptly as you are able at that time.

Thank you so much again. This meeting is adjourned.

[Whereupon, at 4:41 p.m., the subcommittee was adjourned.]