U.S. PIRG
Standing Up
To Powerful Interests

Written Testimony

of

Mike Litt

Consumer Campaign Director

U.S. Public Interest Research Group

For a Hearing on

Improving Data Security at Consumer Reporting Agencies

Before the House Committee on Oversight and Reform's Subcommittee on Economic and Consumer Policy

The Honorable Raja Krishnamoorthi, Chairman

---

26 March 2019

Chairman Krishnamoorthi, Ranking Member Cloud, and Members of the Subcommittee:

Thank you for the opportunity to testify on how to best improve cybersecurity at credit reporting agencies (CRAs). I am the national consumer campaign director for the U.S. Public Interest Research Group (U.S. PIRG). We are an independent non-profit group that promotes consumer rights. I work on identity theft prevention, among other consumer issues. I wrote a report in 2015 called, "Why You Should Get Security Freezes Before Your Information is Stolen,"[1] and I testified before the House Financial Services Committee after the Equifax data breach.[2] I also wrote a report last September called, "Equifax Breach: One Year Later."[3]

In my testimony today, I will outline the need for financial penalties and strong oversight to make sure the CRAs, also known as credit bureaus, are doing everything they can to protect our personal data, which we did not give them permission to collect or sell in the first place. I will also provide recommendations for protecting consumers from identity theft and other fraud.

I. Why the Equifax Breach is the Worst Breach in History

A discussion about improving cybersecurity at the credit bureaus should start with the Equifax breach, which best illustrates the real risk posed to real people when data security is botched at a credit bureau.

On September 7th, 2017, Equifax publicly announced a breach of its data belonging to approximately 143 million American consumers[4]. It later updated that number to 145.5 million[5] and then to nearly 148 million affected Americans[6]. By exposing sensitive personal information, including Social Security numbers and birthdates, and for some people, credit card numbers and driver's license numbers, Equifax put consumers at risk of several types of identity theft and fraud.

We all know credit card numbers can be used to make fraudulent purchases on your existing credit accounts. But what makes the Equifax breach particularly bad is that with your stolen Social Security number and birthdate in hand, an identity thief has the keys to commit new account identity theft and several other types of fraud.

For example, with just your name and Social Security number (SSN), an ID thief can try to apply for new credit cards or loans, order the latest smart phones on payment plans, and open utility accounts in your name. Coupled with your birthdate, a thief could also try to file your taxes, collect your Social Security benefits, and possibly get your healthcare or medical services.

---

[1] Ed Mierzwinski and Mike Litt, U.S. PIRG, *Why You Should Get Credit Freezes Before Your Information is Stolen*, October 2015.
[2] Mike Litt, *Written Testimony of Mike Litt Consumer Advocate, U.S. PIRG: Continuation of Hearing entitled "Examining the Equifax Data Breach" Before the Financial Services Committee*, 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/10.25.2017_mike_litt_testimony.pdf.
[3] Mike litt and Ethan Lutz, U.S. PIRG, *Equifax Breach: One Year Later, How to Protect Yourself Against ID Theft and Hold Equifax Accountable*, September 2018.
[4] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (press release), 7 September 2017.
[5] Equifax, *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident* (press release), 2 October 2017.
[6] Equifax, *Equifax Releases Updated Information on 2017 Cybersecurity Incident* (press release), 1 March 2018.

Add to the mix your driver's license number, which could be used to create a fake ID card, and an identity thief might also try to apply for a job, get insurance, lease an apartment, or even commit crimes in your name.

And as long as Social Security numbers continue to be used to verify our identities, you are at risk of such fraud and the accompanying harm to your finances, reputation, and peace of mind for the rest of your life.

According to the Federal Trade Commission, fraud related to new credit card accounts was the most reported type of identity theft by consumers in 2018, making up 29% of all identity theft reports.[7] This was a 24% increase from 2017.[8] Also, 11,301 consumer complaints to the Consumer Financial Protection Bureau since September 8th, 2017, were categorized as problems with credit inquiries on credit reports not recognized by the consumer, debt as a result of identity theft, or credit cards opened as a result of identity theft or fraud.[9] [10]

II. The Need for Fines and Strong Oversight to Improve Data Security at the CRAs

A. We are Not the Customer

Our relationship as consumers with the credit bureaus does not follow the traditional rules of the marketplace. We are not the customers of the credit bureaus; we are their product. You have no choice over whether they collect your personal information.

That dynamic is precisely why stiff financial consequences for losing our data and strong oversight to prevent data loss in the first place are needed if we want to hold the credit bureaus accountable and make sure they do everything possible to protect our data.

B. The Financial Consequences for Losing Consumer Data Need to be Meaningful

The credit bureaus make money by selling your financial and other histories to their business customers who are deciding whether to extend credit to you, hire you for a job, or insure you. We did not ask or give them permission to collect or sell our personal, sensitive information. The credit bureaus should therefore be held even more accountable for securing our data.

---

[7] Federal Trade Commission, *Consumer Sentinel Network Data Book 2018*, *February* 2019.
[8] Ibid.
[9] This search query includes complaints from September 8, 2017 - March 24, 2019. See Consumer Financial Protection Bureau, *Consumer Complaint Database,* accessed 24 March 2019.
[10] For a sampling of complaint narratives in the CFPB database that give us a better understanding of the personal impacts of identity theft, of which the Equifax breach put consumers at risk, see Appendix C of Mike Litt and Ethan Lutz, U.S. PIRG, *Equifax Breach: One Year Later, How to Protect Yourself Against ID Theft and Hold Equifax Accountable*, September 2018.

In the case of the Equifax breach, there have been Congressional hearings, lawsuits, government investigations, proposed legislation, and a consent order.[11] A House Oversight and Government Reform Committee investigation concluded that the Equifax breach "was entirely preventable."[12]

But so far Equifax still has not paid a price for putting so many consumers in harm's way. And you as a consumer cannot sever your relationship with the company.

That's why the specter of hefty fines is necessary for preventing breaches as bad as the Equifax breach from ever happening again. We should also remember that the breach at Equifax wasn't the first one involving a credit reporting agency. For example, Experian had 15 million files hacked in 2015.[13]

For starters, the FTC should be given authority to issue civil penalties after a first violation of the Gramm-Leach-Blilely Act.[14] Currently, the FTC can only issue a consent order after a first violation of the law and then financial penalties if the order is violated.

There should also be large, mandatory financial penalties for any loss of personal data at credit bureaus that are defined by the CFPB as larger participants.[15] A significant portion of the penalty money should be used to compensate consumers. There should also be mandatory financial penalties for non-compliance with the FTC's Safeguards Rule. Examination and supervision of credit reporting agencies, which is discussed in the next section, is essential for determining compliance with the Safeguards Rule.

C. The CFPB Should Use its Available Authority to Take Action on Data Security

The Consumer Financial Protection Bureau (CFPB) has tools the Federal Trade Commission does not. In addition to greater rule-making authority, these tools include the ability to supervise and

---

[11] Mike litt and Ethan Lutz, U.S. PIRG, *Equifax Breach: One Year Later, How to Protect Yourself Against ID Theft and Hold Equifax Accountable*, September 2018.

[12] U.S. House of Representatives Committee on Oversight and Government Reform, *Committee Releases Report Revealing New Information on Equifax Data Breach* (press release), 20 December 2018, accessed at https://web.archive.org/web/20181210193219/https://oversight.house.gov/report/committee-releases-report-revealing-new-information-on-equifax-data-breach/

[13] Experian, *Experian Notifies Consumers in the U.S. Who May Have Been Affected by Unauthorized Acquisition of a Client's Data* (press release), 1 October 2015.

[14] A joint committee report recommends giving the FTC civil penalty authority for first violations of the law. See The Democratic Staffs of the Committee on Oversight and Government Reform and Committee on Science, Space and Technology, *What the Next Congress Should Do to Prevent a Recurrence of the Equifax Data Breach*, 10 December 2018.

[15] Senators Elizabeth Warren and Mark Warner sponsored legislation during the 115th Congressional session that provides an example of what these mandatory penalties can look like. See The Office of Elizabeth Warren, *Warren, Warner Unveil Legislation to Hold Credit Reporting Agencies Like Equifax Accountable for Data Breaches* (press release), 10 January 2018.

examine companies for compliance with the law and to catch problems before they become worse, and to enforce the law by issuing penalties after a first violation.[16]

The CFPB has exercised robust examination and enforcement authority over larger participant credit reporting agencies, except for in the area of data security.[17]

Authority over CRA data security was retained by the FTC in Section 1031 of the Dodd-Frank Act. Title V of the Gramm-Leach-Bliley Act of 1999 gave the FTC authority to write rules establishing data security responsibilities for non-bank financial firms, including CRAs. The FTC's data security rule is known as the Safeguards Rule.

While the FTC has enforcement authority over its Safeguards Rule, the CFPB has enforcement and examination authority over companies within its jurisdiction for Unfair, Deceptive, or Abusive Acts and Practices (UDAAP).[18]

We know from Equifax's SEC filings that the CFPB is investigating the Equifax breach. In fact, Equifax's recent annual 10-K filing states:[19]

> The staffs of the CFPB and FTC have informed us that their respective agencies intend to seek injunctive relief damages and, with respect to the CFPB, civil money penalties against us based on allegations related to the 2017 cybersecurity incident. We have submitted written responses to the CFPB and FTC addressing their allegations, and we continue to cooperate with the agencies in their investigations.

The CFPB is clearly using its authority to take action on data security in the case of the Equifax data breach - and it should do so more deliberately and regularly with other companies within its jurisdiction. The CFPB should consider and prioritize data security as a factor for which it examines companies.

---

[16] Although FTC can impose penalties for any violation of the FCRA or the Fair Debt Collection Practices Act, it can only impose civil penalties under either its core authority under the FTC Act or its GLBA requirements after a firm is found to be in violation of an FTC-imposed consent decree.

[17] The CFPB published its final rule on defining larger participants in the credit reporting market as part of its non-bank supervision program on July 20th, 2012. The rule defines participants with at least $7 million in annual receipts from consumer reporting activities. See CFPB, *Defining Larger Participants of the Consumer Reporting Market*, 20 July 2012.

[18] As the CFPB explains, the Dodd-Frank Act provides it "with rule-making authority and, with respect to entities within its jurisdiction, enforcement authority to prevent unfair, deceptive, or abusive acts or practices in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service. In addition, the CFPB has supervisory authority for detecting and assessing risks to consumers and to markets for consumer financial products and services." See CFPB, *Unfair, Deceptive, or Abusive Acts or Practices (UDAAPs) Examination Procedures*, 1 October 2012.

[19] Equifax, *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934*, 21 February 2019.

Given the CFPB's infrequent use of its UDAAP authority to take action on data security so far, it would be ideal for Congress to transfer authority over data security under the Gramm-Leach-Blilely Act from the FTC to the CFPB. This transfer would give the CFPB a clear mandate to use its tools, such as supervision, that the FTC does not have to protect consumer data. As the GAO's Equifax report explains, the FTC can only act *after* a data breach has occured because it does not have the authority to examine companies for compliance with the law and to catch problems.[20] The CFPB is the best candidate for such a transfer because it already has a track record of successfully examining the credit reporting agencies in other areas, such as accuracy of credit reports and disputes.[21] Alternatively, Congress could give the FTC supervisory authority under GLBA. That all said, it is important to note that the CFPB already has the authority to take action on data security and does not actually need an act of Congress to use it.

D. Basic Types of Security Measures Should be Required at the Credit Reporting Agencies

Although the FTC's Safeguards Rule requires that certain non-bank financial firms, including CRAs, have an information security program, it is missing basic types of security measures that should be in place.

The FTC's newly proposed amendment to its Safeguards Rule includes some good first steps that would require basic types of security measures, without prescribing specific methods to meet those requirements.[22] **For example, requiring that companies encrypt data, utilize multi-factor authentication[23], and implement controls for who has access to data are basic measures that should be required.**

The House Oversight and Government Reform Committee's report on the Equifax data breach shows that such requirements are needed. The report states that hackers found unencrypted credentials that enabled them to access 48 databases, which allowed them to locate unencrypted personally identifiable information (PII) 265 times.[24] Additionally, Equifax officials identified access controls as one of five major areas of weaknesses that contributed to the breach.[25] [26]

---

[20] GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, August 2018.
[21] For further explanation of this position, see Chi Chi Wu, *Testimony before the U.S. House of Representatives Committee On Financial Services regarding "Examining the Equifax Data Breach,"* 25, October 2017.
[22] FTC, *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules*, 5 March 2019.
[23] One factor might be something secret that only "you know," such as a password, but certainly not your SSN. Another might be something "you have," such as a token. A third factor under consideration might be something "you are," such as your fingerprint or retina scan. See FTC, *Safeguards Rule Federal Register Notice*, 5 March 2019.
[24] House Committee on Oversight and Government Reform, *The Equifax Data Breach*, December 2018, accessed at https://web.archive.org/web/20181210223114/https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf
[25] Ibid.

E. Robust Data Breach Notification Should be Required for the Credit Reporting Agencies

The FTC's Safeguards Rule requires many non-bank financial institutions, including CRAs, to have an incident response plan. However, data breach notifications are not required as part of the plan. The FTC's proposed amendment to its Safeguards Rule includes new requirements for the general areas that should be addressed in a response plan but still does not require breach notification to consumers or to the FTC.[27] The proposed amendment does however seek public input on whether notification should be required to the FTC and to the public.[28]

Breach notification to consumers should be required based on an ***acquisition*** standard, as opposed to a harm trigger. Additionally, breach notification to the FTC and state attorneys general should be required for all breaches.

If information has been lost, it should be presumed to be acquired and therefore require a notification. Harm triggers on the other hand only require notification if the breached entity determines that harm is posed to the individuals whose information was lost. Your right to know if your personal information has been lost should not depend on a determination of harm by the company that lost your information in the first place.

In the absence of federal breach notification laws, all states have stepped in with their own requirements for breach notification.[29] A handful of states, including California and Texas have breach notification laws based on an acquisition standard. A majority of states have notification laws based on a harm trigger, but they do not explicitly limit the definition of harms to financial ones, as we have seen industry groups try to do at the federal level in previous congresses.[30]

Many states have taken the lead with pro-consumer data breach notification laws by expanding the definition of personally identifiable information (PII) to include information such as biometrics; physical and mental health, medical history, and insurance; and username or email address in combination with a password or security question.[31]

---

[26] The Breach podcast looks into various aspects of the Equifax breach. For an account of Equifax's security failures, see Episode 3 of Season 2 of Breach Podcast, *Equifax Data Breach: What Went Wrong*, accessible at https://www.carbonite.com/podcasts/breach/s02e03-Equifax-data-breach
[27] FTC, *Safeguards Rule Federal Register Notice*, 5 March 2019.
[28] Ibid.
[29] Privacy Rights Clearinghouse, *Data Breach Notification Laws: Now in All 50 States*, 09 May 2018.
[30] Ed Mierzwinski, *Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director Hearing on "Identity Verification In A Post-Breach World"*, 30 November 2017.
[31] For examples of states with expanded definitions of PII, see Laura Moy, *Statement of Laura Moy, Deputy Director Center on Privacy & Technology at Georgetown Law Before the U.S. House of Representatives Financial Services Committee Hearing on Continuation of Hearing Entitled "Examining the Equifax Data Breach,"* 25 October 2017.

Congress should reject continued efforts to preempt and replace stronger state laws with a weaker federal one. Any federal law should set the floor, not the ceiling, and allow states to continue innovating their protections to meet future threats posed to consumers.

F. The CFPB Should Make Sure That It Is Looking at All CRAs in the Marketplace and Assessing Whether They Fall within Its Purview

When the CFPB published its larger participant rule for credit reporting agencies in 2012, it estimated from the Economic Census that there were about 410 CRAs in the marketplace, about 30 of which met its threshold of $7 million in annual receipts to qualify as a larger participant and be subject to CFPB supervision.[32]

The CFPB should ensure that it is assessing whether each CRA in the marketplace falls under its larger participant rule.

CRAs should be required to register in a federal registry so that consumers can know which companies might hold information about them and so that the CFPB can make sure it isn't missing any companies that it could be examining.[33]

Short of creating a registry, we urge the CFPB to cross reference its own lists of CRAs with the lists of states, such as New York[34] and Maine[35] [36], where CRAs are required to register with the state if they possess credit files of consumers from those states.

III. Recommendations for Protecting Consumers from Identity Theft and Other Types of Fraud

A. Institute a "Default Credit Freeze"

The best way to protect yourself from new account identity theft, where an ID thief opens an account and racks up a ton of debt in your name, is by getting credit freezes, also known as security freezes, at the three big credit bureaus.[37] Credit freezes stop identity thieves from opening accounts

---

[32] CFPB, *Defining Larger Participants of the Consumer Reporting Market*, 20 July 2012.
[33] The idea for a federal registry of CRAs is further explained in a coalition letter U.S. PIRG signed in response to a Senate request for feedback on data privacy, protection and collection. See National Consumer Law Center et al, *Re: Feedback on Data Privacy, Protection and Collection*, available at https://www.nclc.org/images/Response-to-CrapoBrown-Request-for-Feedback_and_Public_Privacy_Principles.pdf, 15 March 2019.
[34] New York Department of Financial Services, *Consumer Credit Reporting Agency Registration*, accessed at https://www.dfs.ny.gov/consumer/ccra_registration.htm, 24 March 2019.
[35] Maine Bureau of Consumer Credit Protection, *Credit Reporting Agency Licensing Information*, accessed at https://www.maine.gov/pfr/consumercredit/licensing/credit_reporting_agency/licensing.htm, 24 March 2019.
[36] A search of licensees found 46 registered active credit reporting agencies out of 120 applications. See State of Maine, Regulatory Licensing & Permitting, accessed at https://www.pfr.maine.gov/almsonline/almsquery/SearchCompany.aspx, 24 March 2019.
[37] Some news outlets have reported that cell phone companies have opened fraudulent accounts using credit reports provided by the National Consumer Telecom & Utilities Exchange (NCTUE). We therefore

in your name by freezing access to your credit reports - if creditors can't access your credit reports to determine your creditworthiness, they simply won't open a new account.

The best way to protect our data would be to have our credit reports frozen by default so that we can control who has access to our credit reports when we actually want to apply for credit.[38]

B. Remove the Preemption of State Laws from the Current National Credit Freeze

In the absence of a "default credit freeze," the next best thing is for consumers to be able to opt-in for control over their data for free.

Prior to the Equifax data breach, only four states had laws that made getting and removing credit freezes free for consumers.[39] All other states and the District of Columbia had their own laws that allowed the three national CRAs to each charge consumers between $3-10 to get credit freezes and $2-12 to remove them.[40]

In response to the Equifax data breach, 19 states passed laws in 2018 that made getting and removing credit freezes free.[41] Congress followed suit with a free national credit freeze law, as part of S.2155.[42]

Although the new law eliminated credit freeze fees for all consumers, it preempted states with stronger credit freeze laws.[43] For example, some states had credit freezes that applied to checks for employment and insurance, where identity theft can still occur. The national freeze only applies to checks for credit purposes.

We urge Congress to remove the preemption of the national freeze law and allow states to improve on it.[44]

---

also recommend freezing your credit report at NCTUE. See Kathy Kristof, "This Equifax Credit Database Can Boost Your Risk of Phone Fraud," MoneyWatch, 16 May 2018.

[38] In the 115th Congress, we supported S.2362, the Control Your Personal Credit Information Act of 2018, introduced by Senator Reed. We would support a similar defaut credit freeze bill if introduced in the House of Representatives.

[39] Mike Litt, *Written Testimony of Mike Litt Consumer Advocate, U.S. PIRG Continuation of Hearing entitled "Examining the Equifax Data Breach" Before the Financial Services Committee United States House of Representatives*, 25 October 2017.

[40] Mike Litt and Ethan Lutz, U.S. PIRG, *Equifax Breach: One Year Later, How to Protect Yourself Against ID Theft and Hold Equifax Accountable*, September 2018.

[41] Ibid.

[42] 115th Congress, *S. 2155 - Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.

[43] See (b) Conforming Amendment under Sec. 301 of 115th Congress, *S. 2155 - Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.

[44] A discussion draft of this year's Comprehensive Consumer Credit Reporting Reform Act introduced by House Financial Services Committee Chairwoman Maxine Waters removes preemption of state laws from the national free credit freeze. See 116th Congress, *Discussion Draft to Amend the Fair Credit Reporting Act to Improve the Consumer Reporting System, and for Other Purposes*, accessed at https://docs.house.gov/meetings/BA/BA00/20190226/108945/BILLS-116pih-Waters20.pdf, 24 March 2019.

C. Require an Online Method for Requesting Credit Freezes for Protected Consumers

With the passage of S. 2155, Congress also created a right for guardians to request free credit freezes for protected consumers.[45] However, the national CRAs are not required to provide an online method for requesting protected consumer freezes the way they are for all other consumers.[46][47]

The only option available is to mail in a freeze request with sensitive information, including a Social Security number. Controlling access to protected consumers should not be a hassle or security risk.

We urge Congress to require the national CRAs to provide an online method for requesting protected consumer freezes the way they do for all other consumers.

D. Restore Servicemembers' Rights to a Day in Court for Problems with Credit Monitoring

S. 2155 also created a new right for servicemembers to free credit monitoring.[48] However, it denies servicemembers a right to a day in court should something go wrong with the credit monitoring service.[49] For example, if a servicemember becomes a victim of identity theft because the credit monitoring failed to alert them to fraudulent activity, they will be denied their fundamental American right to a day in court. This is the first time that any class of consumer has been denied a day in court to enforce their rights under the Fair Credit Reporting Act.

We urge Congress to restore servicemembers' rights to a day in court to enforce their rights to free credit monitoring under the Fair Credit Reporting Act.[50]

E. Provide Consumers "One Stop Shopping" Control over Their Credit Information

Consumers have numerous rights to control their credit information, but exercising their rights can be confusing and a hassle.

---

[45] A protected consumer is defined as a consumer under the age of 16 or an incapacitated person or protected person who has an appointed guardian. See (j) National Protection For Files And Credit Records Of Protected Consumers under Sec. 301 of 115th Congress, *S. 2155 - Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.

[46] The law establishes time frames for placing protected consumer freezes that are requested electronically. However, the credit bureaus are not providing electronic means for requesting protected consumer freezes, presumably because there is not an explicit requirement for a freeze webpage like there is for all other consumers. See (6) Webpage under Sec. 301 of 115th Congress, *S. 2155 - Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.

[47] For an account of the problems with requesting credit freezes for children, see Ron Lieber, "How Equifax Complicates a Simple Task: Freezing a Child's Credit," *The New York Times*, 8 March 2019.

[48] See Sec. 302 of 115th Congress, S. 2155 - *Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.

[49] See (4) Applicability under Sec. 302 of 115th Congress, *S. 2155 - Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.

[50] A discussion draft of this year's Comprehensive Consumer Credit Reporting Reform Act introduced by House Financial Services Committee Chairwoman Maxine Waters restores servicemembers' rights to a day in court to enforce their right to free credit monitoring. See 116th Congress, *Discussion Draft to Amend the Fair Credit Reporting Act to Improve the Consumer Reporting System, and for Other Purposes*, accessed at https://docs.house.gov/meetings/BA/BA00/20190226/108945/BILLS-116pih-Waters20.pdf, 24 March 2019.

For example, you currently have to visit and navigate through each of the three national credit bureaus' websites to get credit freezes or dispute mistakes on your reports with each bureau. Additionally, there are separate websites for requesting free copies of your credit report and for opting out of receiving prescreened credit offers.

We urge Congress to provide a single portal where consumers can get clear information and one stop access to tools available to them under the law to control their credit information.

Consumers should also be given more control over their information, such as unlimited free access to their credit scores and reports that can also be accessed from such a one stop portal.[51]

Senators Kennedy and Schatz proposed a one stop shopping portal in 2018 as part of a draft Fair and Accurate Information Reporting (FAIR) for Consumers Act. We would support a similar effort in the House of Representatives.

F. Stop Using Social Security Numbers as Authenticators

The reason why the loss of Social Security numbers puts consumers at risk of identity theft and other types of fraud is because SSNs are used as both identifiers AND authenticators for access to personal information and accounts. As the FTC explains, identifiers match you to your file, while authenticators prove who you say you are.[52]

Identifiers can be thought of as usernames, and authenticators can be thought of as passwords.

The problem is that SSNs were never meant to be used as passwords but are being used as such across a variety of platforms and cannot be changed like regular passwords.

The reality is that SSNs will continue to be used as usernames to identify individuals, but they should no longer be used as passwords to gain access to personal information or create and access accounts.

In particular, CRAs should stop allowing creditors to access consumer credit files with simply a name and Social Security number. Identity thieves take advantage of credit bureau procedures, which allow the issuance of credit reports to potential creditors with substantially less verification than consumer requests for their own report. A thief armed only with your SSN can often obtain credit in your name at his address. The thief does not need to provide to the creditor all the answers a consumer must provide a credit bureau to obtain her own report.

We urge Congress to investigate best practices for companies and organizations to replace Social Security numbers as authenticators. But the CRAs should not wait for such an investigation. They can and should stop using SSNs as an authenticator.

G. Educate Consumers about Risks Posed by Data Breaches and Actions That Can Be Taken

Breached entities typically fail to provide consumers the best information or tools for dealing with the specific type of breach involved. For example, Equifax initially offered a package of services after its breach that, at best, only alerts you to identity theft after it has occured. To this day, Equifax

---

[51] Currently, consumers do not have a right to access their credit scores for free. Consumers have a federal right under the law to one free annual copy of their credit report at each of the national CRAs at https://www.annualcreditreport.com

[52] FTC, *Security in Numbers: SSNs and ID Theft*, December 2008.

still has not clearly explained to consumers how they can prevent and detect the different types of ID theft and fraud made possible by its breach.[53]

Confusion over what consumers should do to protect themselves is compounded by the way the CRAs market their paid identity theft services. For example, Equifax sells two products for $19.95 a month that include credit monitoring and what are dubbed "identity theft protection features."[54] However, a lot of what is included in these products is already available for free. For starters, there is no need to pay to *monitor* your credit activity on your reports when you can *stop* activity on your reports altogether for free with credit freezes. Furthermore, the credit report lock, bank and credit card alerts, annual credit report, and fraud alerts that are included with Equifax's paid products are already free to consumers.

Any breach that involves personal information that could be used for fraud or ID theft should require a notice that explains types of identity theft and fraud that consumers are at risk of due to the type of information compromised and a list of actions consumers can take to prevent or detect those types of theft and fraud.[55]

IV. Conclusion

We are not their customers, but Credit reporting agencies possess vasts amounts of our personal data, including the keys to our financial DNA. Therefore, strong financial penalties and oversight are needed to incentivize them to protect our data.

The authorities of the CFPB and FTC should be used and expanded for those purposes. Additionally, we should be given more control over our own CRA data.

Thank you for the opportunity to testify and discuss a range of ideas for improving cybersecurity at the credit reporting agencies. I look forward to working with you.

[53] For a list of steps consumers can take to protect themselves, see Mike Litt, *New Report: How to Protect Consumers 1 Year After Equifax Breach* (press release), accessible at https://uspirg.org/news/usp/new-report-how-protect-consumers-1-year-after-equifax-breach, 6 September 2018.

[54] Equifax, *Equifax Complete Premier*, accessed at https://www.equifax.com/personal/products/credit/monitoring-and-reports/, 24 March 2019.

[55] We continue to support state laws that protect consumers against a broad number of harms. Breach notice requirements should not be limited to fraud or identity theft harms because breaches, for example, could result in harms including stalking and other physical threats.