Testimony before the

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES

regarding

"Examining the Equifax Data Breach"

October 25, 2017

Chi Chi Wu

Staff Attorney

National Consumer Law Center

7 Winthrop Square, 4th Fl.

Boston, MA 02110

617-542-8010

cwu@nclc.org

Testimony of Chi Chi Wu, National Consumer Law Center
Before the U.S. House of Representatives Committee on Financial Services
regarding
"Examining the Equifax Data Breach"
October 25, 2017

INTRODUCTION AND SUMMARY

Mr. Chairman, Ranking Member Waters, and Members of the Subcommittee, thank you for inviting me to testify today regarding the Equifax data breach. I offer my testimony here on behalf of the low-income clients of the National Consumer Law Center.[1]

NCLC has long advocated for stronger reforms to ensure accuracy and fairness in the U.S. credit reporting system. We have testified many times before Congress, including before this Committee, on the need for reform of the credit reporting system to address issues such as unacceptable error rates, the travesty of the automated dispute system used by the credit reporting agencies or "CRAs," the unfair impact of medical debt on credit reports, and the problems with use of credit reports for employment purposes.[2]

In fact, on the day that Equifax announced the data breach, NCLC was testifying against six anti-consumer bills before the Subcommittee on Financial Institutions and Consumer Credit. Ironically, one of the bills under consideration that day (H.R. 2359, the FCRA Liability Harmonization Act) would eliminate punitive damages and limit class action damages under the Fair Credit Reporting Act (FCRA), dramatically reducing the consequences when Equifax and other credit reporting agencies violate the FCRA. We understand that Representative Loudermilk, the lead sponsor of H.R. 2359, has said he will table the bill for now,[3] but we stand ready to vigorously oppose it again if it is moved forward.

---

[1] The National Consumer Law Center is a nonprofit organization specializing in consumer issues on behalf of low-income people. We work with thousands of legal services, government and private attorneys, as well as community groups and organizations, from all states who represent low-income and elderly individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of the damage wrought by abuses from credit reporting agencies from every part of the nation. It is from this vantage point that we supply these comments. *Fair Credit Reporting* (8th ed. 2013) is one of the eighteen practice treatises that NCLC publishes and annually supplements. This testimony was written by Chi Chi Wu, with assistance from Lauren Saunders of NCLC.

[2] *See, e.g.,* An Overview of the Credit Reporting System: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs., 113th Congr. (2014) (testimony of Chi Chi Wu); Use of Credit Information beyond Lending: Issues and Reform Proposals: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs., 113th Congr. (2010) (testimony of Chi Chi Wu).

[3] Zachary Warmbrodt, Finance industry's deregulation drive faces new threat with Equifax, Politico, Sept. 13, 2017, at http://www.politico.com/story/2017/09/13/equifax-finance-industry-deregulation-242634 ("The congressman instructed the committee that 'he would like to see no further action on H.R. 2359, pending a full and complete investigation into the Equifax breach,' according to Loudermilk spokeswoman Shawna Mercer").

I. The Equifax breach

By now, we are all too familiar with the shocking facts of the Equifax data breach, in which thieves were able to steal the Social Security numbers, dates of birth, and other sensitive information for a mind-boggling 145.5 million Americans. This means half of the US population and nearly three-quarters of the consumers with active credit reports are now at risk of identity theft due to one of the worst – if not the worst - breaches of consumer data in American history. These Americans are at risk of having false new credit accounts, phony tax returns, and even spurious medical bills incurred in their good names.

We know about Equifax's incompetent failure to install a simple cybersecurity patch that led to the massive hack. We have seen Equifax repeatedly bungle its response to the data breach, including inserting a forced arbitration clause in the product it initially offered to breach victims for remediation,[4] tweeting out a fraudulent link to a website that spoofed Equifax's own website for breach victims,[5] and having completely insufficient website and telephone resources resulting on long delays for victims seeking information or freezes.[6]

This horrifying data breach has made Americans aware of the anomalous nature of the credit reporting industry. The companies serve a critically important function in the U.S. economy and in the financial lives of Americans. A good credit history is necessary for consumers to obtain credit, and to have that credit be fairly priced. Credit reports are also used by other important decisionmakers, such as insurers, landlords, utility providers, and unfortunately, even employers. Thus, it is no exaggeration to say that a credit history can make or break a consumer's finances.

Yet credit reporting agencies are entirely private companies that are publicly traded, which means their highest duty is to shareholder profit. Furthermore, consumers do not have any leverage over these private companies, unlike most other industries, because market forces do not apply to this industry.

The American consumer is not the customer, but rather the commodity, of the credit reporting agencies. We have no choice but to have our data fed to these companies. We cannot vote with our feet or our purse strings – we cannot choose to avoid Equifax even after this terrible hack if we want a credit card, a car loan, or a mortgage. When late night hosts make jokes about this awful situation,[7] we know this is a problem that everyone is paying attention to.

---

[4] *See* Section IV, below.

[5] Alfred Ng, Equifax Sends Breach Victims to Fake Support Site, CNET.com, Sept. 20, 2017, *at* www.cnet.com/news/equifax-twitter-fake-support-site-breach-victims/.

[6] Rob Lieber, Finally, Some Answers From Equifax to Your Data Breach Questions, N.Y. Times, Sept. 14, 2017, *available at* www.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html ("Some people are waiting until the middle of the night to try to use Equifax's security freeze website and even failing then to get through. It's like trying to get Bruce Springsteen tickets, except nobody wants to see this particular show").

[7] *See, e.g.*, John Oliver, Equifax: Last Week Tonight with John Oliver, Oct. 15, 2017, *available at* www.youtube.com/watch?v=mPjgRKW_Jmk; Stephen Colbert, Equifax Just Equi-F'ed Everyone, The Late Show with Stephen Colbert, Sept. 21, 2017, *available at* www.youtube.com/watch?v=LyIEd5QVkyc.

In addition to the lack of market forces to rein them it, the credit reporting agencies were also insufficiently regulated until recently. Until 2012, their primary regulator was the beleaguered Federal Trade Commission (FTC), which only had the power to take enforcement action when something went wrong and which was outstaffed and outgunned. Private attorneys can sue under the FCRA, but they generally cannot seek injunctive relief,[8] so the companies can pay off the lawsuits as a cost of doing business and not fix their systems.

II. A culture of impunity, arrogance, and exploitation

Due to this insufficient regulation and the lack of consumer choice, the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly. Their idea of a dispute system was a travesty of automation, converting painstakingly written consumer disputes and supporting documentation into two- or three-digit codes and sending only those codes to the creditor or debt collector (the "furnisher") that provided the erroneous information. After the furnisher responded, the credit reporting agencies' main response was to repeat or "parrot" whatever the furnisher claimed. The CRAs always took the side of the furnisher, like a judge that always sides with the defendant. And they often spent minimal resources on disputes -- at one point, Equifax paid a mere $0.57 per dispute letter to a Philippines-based vendor to handle disputes.[9]

The credit reporting agencies also have accuracy rates that are unacceptable. The definitive FTC study on credit reporting errors found that 1 in 5 consumers have verified errors in their credit reports, and 1 in 20 consumers have errors so serious they would be denied credit or need to pay more for it.[10] It is no surprise then that the three credit reporting agencies are often the top three most complained-about companies to the Consumer Financial Protection Bureau (Consumer Bureau), with the vast majority of complaints involving incorrect information on consumers' credit reports.[11]

Furthermore, these problems with accuracy stem fundamentally from a culture where compliance and quality control take a back seat to profits and marketing. A Consumer Financial Protection Bureau report documenting its supervision efforts over the credit reporting agencies noted major deficiencies at the CRAs, such as:[12]

---

[8] National Consumer Law Center, Fair Credit Reporting § 11.12 (8th ed. 2013), *updated at* www.nclc.org/library.

[9] Chi Chi Wu, National Consumer Law Center, Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in Their Credit Reports (Jan. 2009), at 32, *available at* www.nclc.org/images/pdf/pr-reports/report-automated_injustice.pdf.

[10] Federal Trade Comm'n Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 (Dec. 2012).

[11] *See, e.g.*, Consumer Financial Protection Bureau, Monthly Complaint Report, Vol. 21, March 2017, *available at* https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201703_cfpb_Monthly-Complaint-Report.pdf.

[12] Consumer Financial Protection Bureau, Supervisory Highlights Consumer Reporting Special Edition, Issue 14 (Mar. 2, 2017), available at http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

- No programs to test the accuracy of credit reports that the CRAs produced, prompting Consumer Bureau Director Richard Cordray to remark "we were surprised to find that [the CRAs'] quality control systems were either rudimentary or virtually non-existent."[13]
- Insufficient monitoring and re-vetting of furnishers to ensure they were continuing to meet their legal and other obligations. Furnishers were rarely provided with feedback regarding data quality, and were sometimes charged fees for data-quality reports.
- Deficiencies regarding dispute handling, not only in conducting cursory reviews as discussed above, but failing to consistently notify furnishers of disputes and to describe the results of dispute investigations in FCRA-mandated notices to consumers.

From our years of experience with the credit reporting agencies, and as demonstrated by the Consumer Bureau's report, it appears their culture is to cut corners and to underinvest in compliance management and quality control. *A data company that underinvests in accuracy and compliance is likely to be the same company that will underinvest in information security.* The yawning gaps in data security at Equifax probably stem from the same attitude of trying to see how much it could reduce costs and maximize profits. An emphasis on profits over doing the job right is what we believe contributed to this massive data breach at Equifax. Furthermore, Equifax is not alone, as we believe that the other two big credit reporting agencies (Experian and TransUnion) have similar cultures.

III. <u>The credit reporting agencies promote their own products instead of credit freezes</u>

This attitude of impunity has also manifested itself in the credit reporting agencies' aggressive marketing of credit monitoring as the preferred response to data breaches, instead of offering the far more effective measure of credit freezes, also known security freezes. Credit monitoring is not as effective as security freezes because it only informs consumers after the fact when there has been an attempt to open a fraudulent new account using the consumer's personal information– the proverbial shutting the barn door after the horse has left. A security freeze prevents the consumer's stolen information from being used by thieves in the first place.

The reason that credit reporting agencies promote credit monitoring in response to breaches is simple: the CRAs want to establish credit monitoring as the automatic response when a consumer is worried about identity theft. In addition to the revenues from businesses and government agencies, the real pot of gold is when consumers sign up for the paid subscription version of credit monitoring and ID theft prevention products, which cost $5 to $30 per month, generating a whopping $3 billion in profits in 2015 and 2016.[14]

---

[13] Prepared Remarks of Consumer Financial Protection Bureau Director Richard Cordray at the Consumer Advisory Board Meeting, Mar. 2, 2017, available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-consumer-advisory-board-meeting-march-2017/

[14] Government Accountability Office, Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud, GAO-17-254, March 17, at 5, *available at* www.gao.gov/assets/690/683842.pdf. Not all of $3 billion went to the three primary nationwide CRAs, as there are dozens of companies that offer identity theft prevention products. However, identity theft prevention services usually include a credit monitoring component. For example, the GAO noted that all

In fact, the practice of promoting credit monitoring subscriptions was so ingrained that Experian actually refused to provide free credit freezes when it experienced its own data breach. In October 2015, Experian announced that it had experienced a breach in which the Social Security numbers and other personal data of 15 million T-Mobile customers was stolen. Consumer advocates urged Experian to provide free credit freezes to consumers whose information was stolen.[15] Not only did Experian refuse to officially respond to the consumer advocates, an Experian official accidentally copied consumer advocates on an email sent to Experian North America's CEO stating:

> "This is a predictable response from this group. The precedent set for offering free freezes would haunt all beaches going forward. Doing as they request on either count will not satiate their hatred for Experian.
>
> "We should respond with a well articulated letter regarding why a credit freeze is not a credible response for most people. Fraud alerts and monitoring is adequate. It would also allow us to explain that the data won't likely be used, and that we have remediation experts available to help if it is.
>
> "We could turn our response into a good PR approach if done right."

A copy of this email is attached as Attachment A.

Experian deliberately made a choice not to promote the most effective measure against identity theft to consumers who had been victimized by a breach of its own doing. Experian put consumers it had already harmed at risk of identity theft solely to avoid jeopardizing its lucrative credit monitoring business for future breaches.

Indeed, in this most recent breach, Equifax's initial response was to offer one free year of its credit monitoring and identity theft prevention product.[16] But because of intense media scrutiny generated by the massive scale of this breach, consumer advocates and public officials were finally able to get the message out on a large scale that consumers should place credit freezes on their accounts to protect themselves against identity theft. As a result, Equifax initially agreed to provide free credit freezes until November 21, 2017, then to January 31, 2018.[17]

However, even after this massive breach and the intense scrutiny surrounding it, the culture of impunity still remains with the credit reporting agencies. This time around, the credit reporting

---

but 3 of the 26 identity theft service providers it reviewed provided some level of credit monitoring. Thus any provider that is not a CRA must contract with a CRA to provide access to consumer credit reports. *Id.* at 9. Consequently, the CRAs make money even when their competitors sell a subscription product that includes credit monitoring.

[15] Letter from Consumer Advocates to Experian and T-Mobile re: Data Breach, Oct.2, 2015, *available at* www.nclc.org/images/pdf/credit_reports/letter-experian-data-breach-oct2015.pdf.

[16] Press Release, Equifax Announces Cybersecurity Incident Involving Consumer Information, Sept. 7, 2017, *available at* https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[17] FTC, Free credit freezes from Equifax, Sept. 19, 2017 (updated Oct. 5, 2017 to reflect new January 31, 2018 date), *available at* www.consumer.ftc.gov/blog/2017/09/free-credit-freezes-equifax.

agencies are promoting credit "locks" instead of credit freezes. Indeed, in its website, Transunion heavily steers consumers toward its free credit "lock" product and away from freezes, comparing locks and freezes in a very biased manner. For example, TransUnion notes that:[18]

- Lock - You want instant independent control over access to your credit information
- Freeze - You'd rather have TransUnion control access to your credit information

What Transunion neglects to inform consumers is that:

- The "lock" is part of TransUnion's TrueIdentity product. Consumers must agree to an arbitration clause as part of the TrueIdentity product.[19]
- TransUnion generates profits by sending targeted advertising to consumers as part of this product. While this fact by itself is not objectionable, TransUnion fails to point out that this is a drawback to this product in comparison to a security freeze.
- Most importantly, a security freeze is mandated by state law, and there is legal liability if TransUnion fails to comply with the terms of state law. A lock is simply a product offered by TransUnion, and if something goes wrong, the consumer's only remedies are perhaps for breach of contract or unfair practices.

Equifax has announced that it will be offering a free credit lock product for life.[20] It is unclear whether Equifax's credit lock will be associated with an arbitration clause. During testimony before both the House and Senate, former CEO Rick Smith did state there would be no advertising as part of the product. However, he heavily promoted the credit lock product as superior to security freezes without noting the potential drawbacks.

Finally, at least TransUnion and Equifax are offering their lock products without charging a fee. Experian is not offering anything for free.[21] And note that TransUnion or Equifax could decide to stop offering free credit locks at any point, perhaps when the media attention is no longer focused on them, and consumers would have little recourse.

There should be a right to free security freezes for all consumers. After all, this is OUR information in the credit reporting agencies' database, from which they are making billions in profits. Consumers should at least have the control to shut off access to their own information when they are not actively seeking credit. Ideally, a security freeze should be placed on credit reports by default, and access should be turned off until the consumer decides to turn it on.

---

[18] TransUnion, Locking Your Credit Report, *at* www.transunion.com/credit-freeze/place-credit-freeze2 (viewed Oct. 19, 2017).
[19] TransUnion, Service Agreement, *at* www.trueidentity.com/legal/service-agreement (viewed October 21, 2017).
[20] Paulino do Rego Barros Jr., On Behalf of Equifax, I'm Sorry, Wall St. J., Sept. 27, 2017, *available at* www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253.
[21] Ron Lieber, Equifax Calls for Free Credit Locks. Experian's Reply? Nope., New York Times, Oct. 4, 2017, *available at* www.nytimes.com/2017/10/04/your-money/equifax-experian-credit-locks.html.

IV. Use of Forced Arbitration by Credit Reporting Agencies

The credit reporting agencies' culture of impunity is aided and abetted by their use of forced arbitration clauses. Equifax was slow to alert the public to the data breach, but quick to protect itself by attempting to take away consumers' day in court. Buried in the fine print of the website it set up to offer free credit monitoring was a forced arbitration clause and class action ban purporting to apply to any controversy "relating in any way to Your relationship with Equifax" and to be interpreted in "the broadest possible" manner. Equifax eventually relented and removed the clause under intense pressure.[22] But former Equifax CEO Rick Smith, when testifying before the Senate Banking Committee on October 4, admitted that Equifax uses arbitration clauses in other consumer products.[23] Furthermore, it should not be up to the wrongdoer to decide voluntarily if consumers get access to justice, and it should not happen only when a problem is massive enough to generate intense publicity.

Experian and TransUnion also include forced arbitration clauses with class action bans in their products. Experian includes a forced arbitration clause in ProtectMyID.[24] As mentioned above, TransUnion includes one in its TrueIdentity product. The Seventh Circuit criticized TransUnion for one of its arbitration clauses, stating that the company "actively misleads consumers" into thinking that clicking "I Accept" merely authorized TransUnion to obtain information needed to get a credit score, not to force them to give up their day in court.[25]

TransUnion should know the power of class actions to obtain relief for those wrongfully abused, given that it recently lost a lawsuit for carelessly mismatching innocent consumers with suspected criminals and terrorists with similar names on a government watch list. The jury was so appalled by TransUnion's conduct that it ordered the company to pay $60 million ($7,337 for each of the 8,185 class members). Military personnel serving our country abroad were among those mislabeled as potential terrorists or criminals.[26]

A new Consumer Bureau rule will stop these abuses by prohibiting financial companies from putting forced arbitration clauses with class action bans in the fine print of contracts.[27] The rule applies to companies providing credit reports, credit scores, credit monitoring and other services provided to consumers based on information in the consumer's file. But the House of Representatives has voted to repeal the rule and the Senate is considering following suit. This is despite the fact that a recent phone survey conducted by a Republican firm found that, in the

[22] Diane Hembree, Consumer Backlash Spurs Equifax To Drop 'Ripoff Clause' In Offer To Security Hack Victims, Forbes, *available at* www.forbes.com/sites/dianahembree/2017/09/09/consumer-anger-over-equifaxs-ripoff-clause-in-offer-to-security-hack-victims-spurs-policy-change/#2d2a93ef6e7e.
[23] Former Equifax CEO Faces Congress, Wall St. J., Oct. 4, 2017, *available at* https://www.wsj.com/livecoverage/equifax-hack-hearing-1003.
[24] Experian, ProtectMyID® Membership Agreement, Sept. 1, 2015, *at* http://www.protectmyid.com/terms (viewed Oct. 21, 2017).
[25] Sgouros v. Transunion Corp., 817 F.3d. 1029, 1035 (7th Cir. 2016).
[26] James A. Francis, Don't Strip Service Members of Their Right to Join Class-Action Lawsuits, Morning Consult, Oct. 19, 2017, *available at* https://morningconsult.com/opinions/service-members-military-arbitration-fraud-class-action/.
[27] *See* Consumer Financial Protection Bureau, New protections against mandatory arbitration, July 20, 2017, *at* www.consumerfinance.gov/arbitration-rule.

wake of Equifax's massive data breach, the Consumer Bureau's rule has widespread bipartisan support ranging from 64% among Republicans to 74% among Democrats.[28]

V. The need for close supervision

With respect to accuracy and dispute handing, we are finally starting to see modest improvements in the credit reporting agencies. In 2012, American consumers finally got a regulator with the tools, focus, and resources to force the credit reporting agencies to improve their systems – the Consumer Financial Protection Bureau (Consumer Bureau). The Consumer Bureau has started supervising the CRAs by examining their policies, procedures, compliance systems, and employee training. This supervision has begun to start paying by moving the needle on accuracy and dispute issues.[29]

However, Consumer Bureau's supervision is missing a critical element - *it has no mandate to supervise for data security*. When the Dodd-Frank Act created the Consumer Bureau, Congress decided to shift most of the FCRA authority to this new agency, but to keep the identity theft and data security provisions of the FCRA with the FTC. And the major federal law governing data security for the credit reporting agencies – the Gramm Leach Bliley Act - specifically excludes Consumer Bureau from jurisdiction over its data security provisions. *See* 15 U.S.C. §§ 6801(b), 6805(b)(1). While the Consumer Bureau could potentially supervise for data security under other authority, such as the prohibition against unfair, abusive or deceptive practices under Section 1031 of the Consumer Financial Protection Act, the lack of a clear mandate means that the supervision priority has been to focus on issues for which the Bureau does have a mandate – accuracy and dispute handling.

At the time Dodd-Frank was passed, this division of authority might have made sense. But it has resulted in terrible consequences. The FTC has no supervision authority to investigate proactively what is going on inside the credit reporting agencies. The FTC can only react after the fact to this data breach by taking enforcement action. It could not have prevented this tragedy, because it could never get inside the guts of the credit reporting companies to make sure their data security was adequate and compliant.

We believe the Gramm-Leach-Bliley data security authority should be transferred over to the Consumer Financial Protection Bureau. The Bureau can make data security part of its current supervisory efforts and force the companies to fix their systems before there is another terrible breach. The Consumer Bureau has the infrastructure and resources to dig deep into the procedures and policies of these companies on data security. We need the most effective regulator – the only one examining the credit reporting agencies – to be in charge of making sure the CRAs properly invest in data security.

---

[28] Sylvan Lane, GOP polling firm: Bipartisan support for consumer bureau arbitration rule, The Hill, Oct. 5, 2017, *available at* http://thehill.com/policy/finance/354143-gop-polling-firm-finds-bipartisan-support-for-consumer-bureau-arbitration-rule.

[29] In addition, a settlement obtained by a multistate group of Attorneys General with the credit reporting agencies also requires the agencies to improve dispute handling and accuracy procedures. Assurance of Voluntary Compliance/Assurance of Voluntary Discontinuance, In the Matter of Equifax Info. Serv. L.L.C., Experian Info. Solutions, Inc., and TransUnion L.L.C. (May 20, 2015).

VI. Necessary reforms

Congress should adopt some fundamental immediate reforms in response to the Equifax data breach:

- **Consumers should not be forced to pay for security freezes under any circumstances, much less after they have been victimized by a data breach.** That's why we have supported several bills to mandate free security freezes. Free security freezes are also a component of H.R. 3755, the Comprehensive Credit Reporting Reform Act, sponsored by Ranking Member Maxine Waters.

- **The Consumer Financial Protection Bureau should be given the authority over the data security standards under the Gramm Leach-Bliley Act and the FCRA so that it has a clear mandate to supervise the credit reporting agencies regarding this area.**

- **The Internal Revenue Service (IRS) should make identity protection personal identification numbers (PINs) available to everyone.** The Equifax breach has put 145.5 million Americans at risk of other types of identity theft, such as tax refund identity theft, in which crooks file phony tax returns using consumers' names and identifiers, then steal the refund. The only method to prevent tax identity theft is an Identity Protection PIN from the IRS, but the IRS only makes PINs available to prior victims of identity theft and to consumers in Florida, Georgia, and the District of Columbia. Thus, we have urged IRS to make Identity Protection PINs available to all affected breach victims[30] and Congress should make a similar demand.

- **Congress should enact wider reforms of the credit reporting industry**. This data breach has very much highlighted the problems with and abuses by credit reporting agencies, and these should all be addressed. That is why we strongly support H.R. 3755, the Comprehensive Credit Reporting Reform Act, and we thank Ranking Member Waters for introducing it.

Finally, we agree with commentators who have suggested that a new paradigm for credit reporting might be necessary. We want to make clear that we are not urging the elimination of Equifax, because frankly the other two credit reporting agencies are as equally flawed. Indeed, Equifax has exhibited some remorse and apologized, but as demonstrated above, TransUnion and Experian have not changed their attitude at all and are still engaged in less than forthright tactics.

Some commentators have urged that credit reporting be a public function, or that we nationalize the CRAs. Those ideas are worth exploring and studying. For example, credit reporting could be a function of government-sponsored enterprises, similar to the role of Fannie Mae and Freddie Mac in the mortgage market.

[30] Letter from consumer and tax attorneys urging IRS to make Identity Theft PINs available to all taxpayers, Sept. 21, 2017, *available at* www.nclc.org/images/pdf/credit_reports/irs-lttr-re-efx-breach.pdf.

Conclusion

The massive theft of sensitive personal information for half of all Americans demands a real and meaningful response by Congress. Some media outlets have speculated Congress will do nothing more than make public displays of outrage at Equifax. We urge this Committee to prove them wrong.

Thank you very much for the opportunity to testify today. I would be happy to answer any questions.

NCLC®

Chi Chi W u <cwu@nclc.org>

Re: Consumer Groups Call on Experian and T -Mobile to Provide Free Security Freezes to Hacked Customers

1 message

Hadley, Tony Fri, Oct 2, 2015 at 2:48 PM
To: Chi Chi Wu
Cc: "john.legere, "Boundy, Craig"

This is a predictable response from this group. The precedent set for offering free freezes would haunt all beaches going forward. Doing as they request on either count will not satiate their hatred for Experian.

We should respond with a well articulated letter regarding why a credit freeze is not a credible response for most people. Fraud alerts and monitoring is adequate. It would also allow us to explain that the data won't likely be used, and that we have remediation experts available to help if it is.

We could turn our response into a good PR approach if done right.

Thoughts?

I would be happy to draft an initial response.

Tony

Sent from my iPhone

On Oct 2, 2015, at 11:15 AM, Chi Chi Wu wrote:

> Dear Mr. Boundy and Mr. Legere: Please see the attached letter, the text of which is also copypasted below.
>
> October 2, 2015
>
> Craig Boundy — John Legere
> CEO — CEO
> Experian North America — T-Mobile US
>
> Dear Mr. Boundy and Mr. Legere:
>
> The undersigned consumer advocacy and labor groups write to you regarding the recent announcement that there has been a massive security breach of T-Mobile customer data from Experian. We understand from media reports that over 15 million consumers may have had their sensitive personal information, including Social Security Numbers and other identifying numbers (such as driver's license information), stolen by hackers.
>
> The media stories also report that Experian and T-Mobile are offering free credit monitoring for two years in response to the security breach. We are writing to urge that, in addition, Experian and T-Mobile should offer free security freezes to all affected customers, for all three major credit bureaus. Otherwise, affected consumers could be charged up to $15 per credit bureau.

As you know, a security freeze is the most effective measure against identity theft involving the opening of new credit accounts, and is certainly advised here given the highly sensitive information that was stolen. Credit monitoring only informs consumers after the fact when there has been an attempt to open a fraudulent new account using the consumer's personal information– the proverbial shutting the barn door after the horse has left. A security freeze prevents the consumer's stolen information from being used by thieves in the first place.

Finally, we urge that Experian remove its mandatory arbitration provision from its credit monitoring agreement for the affected customers, and for all customers of its credit monitoring products. It's bad enough that Experian has allowed hackers to infiltrate its computer systems; to then slip in a provision in the credit monitoring agreement that deprives these victimized consumers of their legal remedies against Experian is unconscionable.

If you have any questions about this letter, please contact Chi Chi Wu at 617-542-8010 or cwu@nclc.org.

Sincerely,

National Consumer Law Center (on behalf of its low-income consumers)

Communications Workers of America, CWA

Consumer Action

Center for Digital Democracy

Center for Economic Justice

National Association of Consumer Advocates

U.S. PIRG

Woodstock Institute

Housing Resources of Columbia County

<Experian Oct 2015 Data Breach letter.pdf.secure>