Loyola Consumer Law Review

Volume 30 | Issue 3 Article 6

2018

The Equifax Breach: What We Learned and How We Can Protect Consumer Data

Thomas G. Siracusa Jr

THE EQUIFAX BREACH: WHAT WE LEARNED AND HOW WE CAN PROTECT CONSUMER DATA

*Thomas G. Siracusa Jr.**

I. INTRODUCTION

Consumer credit history reports contain information from three different credit reporting agencies ("CRAs")[1]: Equifax, Experian, and Transunion.[2] Each CRA collects the same information but processes and reports it differently.[3] Their primary purpose is to research and sell consumers' credit information to various creditors.[4] Consumer information collected consists of identity and payment information, records of employment, previously requested credit history reports by creditors, and public records (such as bankruptcies and foreclosures).[5] In May 2017, Equifax experienced a massive data breach that exposed the sensitive information of approximately 145 million Americans.[6] Information obtained by the hackers included full names, birthdates, Social Security numbers, credit card numbers, and driver's license numbers.[7] No information was released to the public concerning the breach until six weeks following the data breach.[8]

---

* J.D. Candidate, May 2019, Loyola University Chicago School of Law.

[1] Latoya Irby, *Who Are the Major Credit Reporting Agencies?*, THE BALANCE (Apr. 8, 2018), https://www.thebalance.com/who-are-the-three-major-credit-bureaus-960416.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Seena Gressin, *The Equifax Data Breach: What to Do,* FEDERAL TRADE COMMISSION (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[7] *Id.*

[8] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14,

The Equifax breach ("Breach") reopened the discussion of consumer data protection. Yet, months after learning about the data Breach, the government has not implemented new data security laws. Data theft is a serious issue. The consequences on consumers include denial of credit and loans, diminished job prospects, higher insurance rates, and even false criminal records.[9] Today, consumers are left to their own credit protection efforts. After the data breach, consumers raced to have their files locked, but CRAs often responded to these requests with time consuming obstacles or denials.[10] CRAs made minimal efforts to mitigate the issue.[11] Equifax finally released an application in January 2018 that allows consumers to lock (or freeze) and unlock their files for free; yet these features were only available once applicants consented to terms that allowed Equifax to continue to store and share consumer information with third parties in limited circumstances.[12] Transunion and Experian offered similar services, but required consumers to sign a class action waiver or pay $9.99 per month.[13] While CRAs made meager efforts to ramp-up data protection, companies like Equifax continued to face criticism from the security community for allowing an easily preventable Breach by ignoring warnings of flaws in their security software.[14] People also blamed the government for the lack of national standards for CRAs with respect to monitoring, security protocols, and imposition of penalties.[15]

2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[9] Bob Sullivan, *9 Surprising Ways Identity Theft Can Hurt You*, CREDIT (June 13, 2014), http://blog.credit.com/2014/06/surprising-ways-identity-theft-can-hurt-you-85080/.

[10] Fred O. Williams, *5 months after Equifax Breach, no new data security rules*, CREDIT CARDS (Feb. 16, 2018), https://www.creditcards.com/credit-card-news/equifax-breach-no-new-data-security-rules-five-months-later.php#bills.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Newman, *supra* note 8.

[15] Heidi N. Moore, *Why Didn't Equifax Protect Your Data? Because Corporations Have All the Power*, THE WASHINGTON POST (Sept. 21, 2017), https://www.washingtonpost.com/news/posteverything/wp/2017/09/21/why-didnt-equifax-protect-your-data-because-corporations-have-all-the-power/?utm_term=.6cbdc1cf6595.

In addition to shedding light on the security concerns accompanying the collection and distribution of consumer credit information, the Breach exposed the truth about the relationship between consumers and corporations. CRAs hold a disproportionate amount of power, with respect to contractual terms and communication, over consumers.[16] More disturbing is that CRAs, which hold vast amounts of data on millions of Americans, often negligently maintain cybersecurity protocols.[17] Fortunately, this negligence and operational problems common with many CRAs became glaringly obvious due to the Breach and thus did not go unnoticed by the government. In September 2017, Senators Elizabeth Warren (D-MA) and Brian Schatz (D-HI) introduced the Freedom from Equifax Exploitation Act ("FREE") in an effort to give consumers more control over credit and personal information.[18] In January 2018, Senator Warren and Senator Mark Warner (D-VA), introduced the Data Breach Prevention and Compensation Act ("DBPC").[19] The objective of the DBPC Act is to initiate heightened authority to supervise CRAs and hold them accountable for breaches involving consumer data.[20] While these bills will not prevent all cases of data theft, they address the key problems associated with CRAs and provide incentives to adequately protect consumer data.[21]

Part II of this Note will provide an overview of the cause of the Equifax breach. Part III will discuss the harmful business practices of CRAs and will highlight the current issues with data security and the importance of data protection legislation reform. Finally, Part IV will cover legislative remedies and include a discussion of the FREE Act and DBPC Act, their potential for reducing the risks of future massive data breaches as well as their potential shortcomings.

---

[16] *Id.*

[17] Newman, *supra* note 8.

[18] Freedom from Equifax Exploitation Act, S. 1816, 115th Cong. (2017) (hereinafter "FREE Act").

[19] Data Breach Prevention and Compensation Act, S. 2289, 115th Cong. (2018) (hereinafter "DBPC Act").

[20] *Id.*

[21] FREE Act, *supra* note 18; DBPC Act, *supra* note 19.

II. THE EQUIFAX DATA BREACH

The Equifax breach raised the question of whether companies electronically storing consumer data take adequate security measures to protect that data. Equifax confirmed many consumers' worst fears when they announced in May 2017 that their system had been hacked via a web application vulnerability; a vulnerability that could have been fixed with a patch that was available two months prior to the Breach.[22] Equifax's negligence was further evidenced by a statement by The Apache Software Foundation ("Apache"), the provider of the computing platform that Equifax and many other enterprises used, which warned its users of the system's vulnerability. Apache confirmed that they had also provided instructions about protection for the vulnerability in March 2017.[23] Following the Breach, Apache speculated that the March 2017 vulnerability was to blame.[24] According to Apache, most data breaches are caused by failing to update software components that have known vulnerabilities.[25] Further, a separate security analytics firm concluded that Equifax was hacked because the company failed to follow Apache's advice and instruction on protections.[26]

To state it plainly, Equifax had two months to take precautions that would have protected the data of 145 million Americans but ignored the warnings.[27] Researchers concluded it was relatively easy to exploit the vulnerability in Equifax's servers and network once discovered.[28] The security community questioned why Equifax had failed to heed warnings and protect their consumers' data. How could a company with such a high level of cybersecurity responsibility allow this to happen? The answer to this question traces back to the ways that CRAs, like Equifax, typically have treated consumers.

---

[22] Newman, *supra* note 8.

[23] *Id.*

[24] *Id.*

[25] René Gielen, *Apache Struts Statement on Equifax Security Breach*, THE APACHE SOFTWARE FOUNDATION BLOG (Sept. 9, 2017), https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax.

[26] Newman, *supra* note 8.

[27] *Id.*

[28] *Id.*

III. CRA'S MISTREATMENT OF CONSUMERS

The CRAs' consumer-corporate relationship is one-sided and ill-defined.[29] In fact, the three major CRAs are among the top three most complained about companies in America.[30] Most of the complaints arise due to erroneous credit reports.[31] In 2012, the Federal Trade Commission ("FTC") conducted a study of credit reports and found that 26% of consumers found at least one error in their file and 5% found critical errors that could lead to a denial of credit or increased insurance rates.[32] Making matters worse, Equifax is known to lack a proper customer service infrastructure.[33] Customers calling to fix an issue with their file experience long wait times and numerous automated prompts.[34] Representatives are reported to be unhelpful and give bureaucratic responses.[35] Some people claim that the process takes weeks before their issues are resolved.[36]

When the Breach was first announced, customers who submitted inquiries about their information were met with the same unresponsiveness that is typical of Equifax customer service.[37] Furthermore, it was this characteristic unresponsiveness that deterred many consumers from contacting Equifax following the Breach.[38]

---

[29] Bobby Allyn, *How the Careless Errors of Credit Reporting Agencies are Ruining People's Lives*, THE WASHINGTON POST (Sept. 8, 2016), https://www.washingtonpost.com/posteverything/wp/2016/09/08/how-the-careless-errors-of-credit-reporting-agencies-are-ruining-peoples-lives/?utm_term=.ffb7d98b7df4/.

[30] 2016 CFPB MON. COMP. REP. VOL. 11., https://files.consumerfinance.gov/f/documents/201605_cfpb_monthly-complaint-report-vol-11.pdf (last visited Apr. 25, 2018).

[31] Allyn, *supra* note 28.

[32] FTC REPORT TO CONGRESS UNDER SECTION 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 1, 26 (2016).

[33] Ron Lieber, *'Dear Equifax: You're Fired.' If Only It Were That Easy*, N.Y. TIMES (Oct. 6, 2017), https://www.nytimes.com/2017/10/06/your-money/credit-scores/equifax-hack.html.

[34] *Id.*

[35] *Id.*

[36] Allyn, *supra* note 28.

[37] Moore, *supra* note 15.

[38] *Id.*

In fact, only around 15 million people visited Equifax's website in the wake of the Breach, compared to the 145 million people affected by it.[39] It was Equifax's poor customer service infrastructure which kept millions of Americans in the dark and fearing for their financial futures.

Failing to provide customers with quality information following the Breach was not the extent of Equifax's negligent behavior. Two and a half months elapsed between the company leaning about the vulnerability in their system and notifying the public about the Breach.[40] In addition, two weeks before consumers were notified, two top Equifax executives sold millions of dollars' worth of their own company stock.[41] Equifax created a website before the announcement that was intended to update consumers on the situation, but directed many people to a fake version, which was supposedly an accident.[42] Equifax's "solution" that followed was to create a website that allowed consumers to enter their Social Security numbers to determine if their information was compromised.[43] However, the website proved to be another sham that generated the same results for everyone.[44] Equifax ended their lackluster efforts with the release of the aforementioned file lock application.[45]

The Breach exposed the way CRAs take advantage of consumers as intermediaries in nearly all of their financial transactions.[46] Our financial system is structured so that consumers are often at the mercy of financial firms, who unilaterally set the rules.[47] Many people, like in the case of the data breach, are unaware that they are in privity with CRAs until something goes wrong.[48] The file lock options mentioned in Part I that the three CRAs offered

[39] *Id.*
[40] Newman, *supra* note 8.
[41] Moore, *supra* note 15.
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] Williams, *supra* note 10.
[46] Moore, *supra* note 15.
[47] *Id.*
[48] *Id.*

post-Breach, demonstrates that contractual terms for ordinary consumers invariably favor the company.[49] Contracts for ordinary consumers are often tailored to prevent negotiation and legal action.[50] Essentially, the contracts serve to eliminate consumer interference with the CRAs' business.[51] On the other hand, contracts between CRAs and other financial firms or wealthy individuals accommodate the latter's personal concerns.[52] The CRAs' primary concern is to profit, so they naturally give more attention to their deep-pocketed customers like banks, mortgage lenders, and credit card companies.[53] While CRAs negotiate with their wealthy customers; they hang consumers out to dry, making them sign away their rights and failing to provide responsive action to protect consumer data.[54] This negligent behavior needs to be stopped. It is clear that CRAs will not police themselves, as market forces do not incentivize them to do so.[55] We need the implementation of laws and regulations to effectuate change.

IV. LEGISLATIVE REMEDIES

Despite being responsible for maintaining the data of hundreds of millions of Americans, CRAs are not federal agencies and have no government affiliation. Federal laws, like the Fair Credit Reporting Act ("FCRA") give consumers limited rights to fix inaccuracies on CRA-generated credit reports and for access to their credit histories.[56] The bill also imposed identity-theft-notification obligations on CRAs.[57] Some states, like Illinois, have more stringent laws.[58] The Illinois Personal Information Protection Act ("IPIP") requires companies that hold their customers' personal data to have maintainable and reasonable security measures to

[49] Williams, *supra* note 10.
[50] *Id.*
[51] Moore, *supra* note 15.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] Fair Credit Reporting Act 15 U.S.C. § 1681 1, 50 (2012).
[57] *Id.*
[58] 815 Ill. Comp. Stat. 530 (2006).

protect data from unauthorized access.[59] However, these laws were not enough to put an end to the negligent behavior of CRAs. The U.S. needs to take additional measures, such as uniformity in standards that will keep CRAs in check and hold them accountable when their data is compromised.

Thankfully, the Breach attracted government attention. In September 2017, the Department of Justice[60] and FTC[61] announced separate investigations of possible corporate malfeasance on the part of Equifax executives. However, federal investigations are often an arduous process and have a reputation for losing the public's attention.[62] Another option is to pursue litigation. Litigation has been offered to help deter CRAs from poor practices.[63] Since the Breach, more than thirty lawsuits have been filed against Equifax resulting in what has the potential to become the largest class action in U.S. history.[64] But lawsuits, at best, typically result in gradual progress and, as Part I explained, many consumers have signed away their rights to bring CRAs into court.[65]

The most effective way to restore consumer rights under these circumstances is through federal legislation. Congress responded to the Breach by the introduction of two bills: the FREE Act,[66] and the DBPC Act.[67] Under these two bills, CRAs like Equifax will be required to maintain reasonable cybersecurity protection standards and response protocols crafted by their regulators in the event of a data breach.[68]

---

[59] *Id.*

[60] Tom Schoenberg et al, *Equifax Stock Sales are the Focus of U.S. Criminal Probe*, BLOOMBERG (Sept. 18, 2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe.

[61] David McLaughlin et al., *FTC Opens Investigation into Equifax Breach*, BLOOMBERG (Sept. 14, 2017), https://www.bloomberg.com/news/articles/2017-09-14/equifax-scrutiny-widens-as-ftc-opens-investigation-into-breach.

[62] Lily Hay Newman, *How to Stop the Next Unstoppable Mega-breach—Or Slow It Down*, WIRED (Sept. 12, 2017), https://www.wired.com/story/how-to-stop-breaches-equifax/.

[63] *Id.*

[64] Moore, *supra* note 15.

[65] Williams, *supra* note 10.

[66] FREE Act, *supra* note 18.

[67] DBPC Act, *supra* note 19.

[68] *Id.*

A. The Freedom from Equifax Exploitation Act

The provisions of the FREE Act require CRAs to offer consumers prompt freezes of their credit files without any fees.[69] CRAs must send one free credit report to consumers each year[70] and offer fraud protection alerts.[71] Even when files are locked, CRAs sell consumer information to companies that seek to target their marketing.[72] The FREE Act prohibits CRAs from profiting off of consumer files while they are frozen.[73] Finally, the bill mandates that fees, which were imposed on consumers to lock their files in the wake of the Equifax breach, to be fully refunded.[74]

Just as the title suggests, the bill aims to acknowledge and penalize the negligent behavior of Equifax and other CRAs in response to the Breach. The objective is simple: consumer control over their own information. Consumers should not be required to pay every time they want to see their personal credit files. People should not have to pay to stop CRAs from allowing third parties to access their information. Consumers should be able to inquire about their files if they are suspicious that an unauthorized user has accessed them. CRAs make hundreds of millions of dollars each year selling their services to creditors.[75] CRAs should not be allowed to continue profiting off of consumer information when they are explicitly told not to use it. Finally, CRAs should not profit off of something that was their fault to begin with. The bill efficiently highlights ways that CRAs wrongfully profit off of consumers and sanctions them. CRAs should profit as intermediaries to the extent that they share information only when it is necessary for consumer

---

[69] FREE Act, *supra* note 18, § 4.

[70] *Id.* § 3.

[71] *Id.*

[72] Elizabeth Warren, *Warren, Schatz Introduce Legislation to Give Control of Credit Information Back to Consumers, Protect Personal Data Following Equifax Hack*, U.S. SENATE (Sept. 15, 2017), https://www.warren.senate.gov/newsroom/press-releases/warren-schatz-introduce-legislation-to-give-control-of-credit-information-back-to-consumers-protect-personal-data-following-equifax-hack.

[73] FREE Act, *supra* note 18, § 4.

[74] *Id.* § 6.

[75] Moore, *supra* note 15.

approval for mortgages, credit cards, or other financial arrangements.

The FREE Act could create some controversy. The bill promotes seemingly limitless credit freezes.[76] Consumer access to credit is tantamount to the well-being of the economy.[77] If consumers were to take advantage of the free service by continuously locking their files for prolonged periods of time, it could create issues.[78] For example, lenders rely on credit files to provide assurance that the consumers applying for their services will not default on loans.[79] Without giving creditors file access, consumers could find their access to credit seriously curtailed, as creditors would feel less confident in consumers' ability to make timely payments on bills or loans.[80] Activities such as purchasing homes and applying for health care could become much more arduous.[81] The bill should be amended to limit the number of times consumers can freeze their credit files per year or the duration of the freezes. Alternatively, consumers should be wary and make sure that their credit history is accessible by appropriate inquiries about their files. During the process of protecting consumer data, it is important that consumers do not begin to disrupt markets and create disadvantages for businesses and themselves.

B. The Data Breach Prevention and Compensation Act

The DBPC Act is a more comprehensive, common-sense approach to securing consumer data.[82] The bill would develop an office of cybersecurity and appoint a director at the FTC tasked with annual inspections and supervision of cybersecurity at CRAs.[83] The bill would allow the FTC to impose new data security

---

[76] FREE Act, *supra* note 18, § 4.

[77] Veronique de Rugy, *Warren's Regulatory Expansion Is Wrong Answer to Equifax Breach*, REASON (Dec. 21, 2017), http://reason.com/archives/2017/12/21/warrens-regulatory-expansion-is-wrong-an.

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] DBPC Act, *supra* note 19.

[83] *Id.* § 3.

standards upon CRAs.[84] Since CRAs currently face no penalties for allowing consumer data to be stolen, the bill would impose strict-liability penalties for breaches.[85] The penalties would begin with a base of $100 for each consumer who had one piece of personal information compromised. An additional $50 for each extra piece of compromised information per consumer.[86] The penalties are capped at 50% of the CRAs' gross revenue from the prior year.[87] However, in cases where the offending CRA experiences a breach and failed to maintain FTC standards or timely notify the FTC of a breach, the per-consumer penalties would double and the penalty cap would increase to 75% of the CRAs' gross revenue from the prior year.[88] Finally, the bill requires the FTC to allocate 50% of its collected penalties to compensate consumers and 50% to reinvest in the cybersecurity office.[89]

If the DBPC Act was in place during the Equifax breach, the CRAs would have paid approximately $1.5 billion in fines.[90] The bill aggressively aims to adjust the financial incentives that cause CRAs to treat consumers negligently. Putting CRAs under the microscope of a governmental regulatory authority would help ensure consumers that their interests are being protected in transactions between financial firms. Given CRAs' current focus on profit, the massive and mandatory penalties that threaten CRAs for failure to comply with FTC regulations would help maintain adequate cybersecurity measures. Compensating consumers after data breaches would remind CRAs that their consumers are just as important to their business as creditors and there is no incentive to treat them negligently.

The DBPC Act also has some potential shortcomings. The

---

[84] *Id.*

[85] *Id.* § 4.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] Elizabeth Warren, *Warren, Warner Unveil Legislation to Hold Credit Reporting Agencies Like Equifax Accountable for Data Breaches*, U.S. SENATE (Jan. 10, 2018), https://www.warren.senate.gov/newsroom/press-releases/warren-warner-unveil-legislation-to-hold-credit-reporting-agencies-like-equifax-accountable-for-data-breaches.

first issue is with some of the bill's language. The bill defines "covered breach"[91] as any instance in which at least one piece of personally identifying information is exposed or is reasonably likely to have been exposed to an unauthorized party.[92] This language is vague. What constitutes the first and additional pieces of information? What does "reasonably likely to have been exposed" mean? The bill also fails to explain how somebody demonstrates their information was reasonably likely to have been exposed. Moreover, the bill does not address whether companies, such as marketing agencies, who receive data from CRAs without consumer knowledge constitute an unauthorized party.[93] If the Equifax breach unveiled anything, it is that everyone's data could have already been compromised. That means their information is already in the hands of unauthorized parties. These are details that need to be clarified in order to create make a more practical piece of legislation. We do not want to open the floodgates for numerous meritless actions that the bill's ambiguous language might allow.

It is unclear how the government would pay each consumer their portion of the penalties CRAs would pay in the event of a data breach.[94] There needs to be more specificity in the plans to identify and compensate affected consumers. However, compensating consumers as the bill provides might not be a sufficiently equitable remedy in many cases. For example, Sen. Warren estimated that under the DBPC Act, Equifax would have had to pay $1.5 million in penalties for the breach.[95] If 50% of the penalties were allocated amongst the approximately 145 million affected consumers, each affected consumer would receive roughly $5. This is not an adequate remedy for somebody whose credit was potentially ruined. An adequate response to this issue is that the bill's primary objective is to prevent data breaches, not punish CRAs or make consumers whole.

Finally, the DBPC Act should not vest complete regulatory

---

[91] DBPC Act, *supra* note 19, § 2.

[92] *Id.*

[93] Moore, *supra* note 15.

[94] Ron Shevlin, *Save Us from the Data Breach Prevention and Compensation Act*, INSIGHT VAULT (Jan. 10, 2018), https://www.crnrstone.com/insight-vault/2018/01/10/save-us-data-breach-prevention-compensation-act/.

[95] Warren, *supra* note 88.

authority of CRAs in the FTC.[96] Cybersecurity is an issue that affects a number of industries, not just those within the scope of the FTC's authority.[97] If the government wanted to address subsequent cybersecurity issues within other industries, they would have to establish more cybersecurity offices within their respective agencies.[98] Government agencies are only allowed to regulate industries to the extent they fall under the general scope of the human activity there are designed to regulate.[99] Having multiple cybersecurity regulators may lead to confusion in determining correct compliance standards, and in some instances create regulatory overlap issues[100] Perhaps a better alternative would be to establish an independent cybersecurity agency that has authority over all industry cybersecurity matters. This would eliminate potential issues with regulatory overlap and industry compliance. CRAs' cybersecurity practices may require different regulation than, for instance, those of internet service providers. Thus, under this arrangement, an independent cybersecurity agency would be able to address a wide array of human activities and issue standards both uniform and unique to particular services.

V. CONCLUSION

The U.S. has a data breach problem and the issue lies with CRAs who put profit over people. The Equifax breach was an example of how bad things can become for consumers when CRAs operate in a manner that exposes consumer data. Federal investigations and lawsuits will not put an end to the negligent behavior CRAs engage in on a national scale. Comprehensive legislation setting a uniform standard for how CRAs operate and interact with the consumers whose data they harbor is necessary. Despite poten-

---

[96] Shevlin, *supra* note 91.

[97] *Id.*

[98] *Id.*

[99] EPA, *The Basics of Regulatory Practice*, ENVIRONMENTAL PROTECTION AGENCY, https://www.epa.gov/laws-regulations/basics-regulatory-process, (last visited Apr. 25, 2018).

[100] *Id.*

tial shortcomings, the FREE and DBPC Acts should allow the government to hinder data thieves from stealing consumer information by keeping a watchful eye on CRAs' business practices, paving the way for additional legislative remedies. Neither of the bills have been brought to the Senate floor, but each have received multiple endorsements from fellow Senators and consumer interest groups.[101] The U.S. needs to take action sooner rather than later. Under the FREE Act, the Senators should consider curtailing the amount of times consumers can freeze their credit files. With respect to the DBPC Act, Congress could consider provisions for extra damages for consumers and creating an independent cybersecurity agency to set harmonized cybersecurity standards and avoid regulatory confusion. The information that CRAs hold is far too sensitive to continue to be poorly safeguarded.

[101] Warren, *supra* note 88.