

1 BRIAN S. KABATECK (152054)  
bsk@kbklawyers.com  
2 NATALIE S. PANG (305886)  
np@kbklawyers.com  
3 KABATECK BROWN KELLNER  
644 South Figueroa Street  
4 Los Angeles, California 90017  
Telephone: (213) 217-5000  
5 Facsimile: (213) 217-5010

6 Attorneys for Plaintiffs and the Proposed  
Classes

7  
8 **UNITED STATES DISTRICT COURT**  
9 **CENTRAL DISTRICT COURT OF CALIFORNIA**  
10 **SOUTHERN DIVISION**

11 WENDY and ROY DURAN, on  
behalf of themselves, and all others  
12 similarly situated,  
13 Plaintiffs,  
14 vs.  
15 EQUIFAX, INC.; and DOES 1 to 10,  
16 inclusive,  
17 Defendants.

) CASE NO.  
) **CLASS ACTION COMPLAINT FOR:**  
) 1) **WILLFUL VIOLATION OF THE**  
) **FAIR CREDIT REPORTING ACT;**  
) 2) **NEGLIGENT VIOLATION OF**  
) **THE FAIR CREDIT REPORTING**  
) **ACT;**  
) 3) **NEGLIGENCE;**  
) 4) **NEGLIGENCE PER SE;**  
) 5) **VIOLATION OF THE**  
) **CALIFORNIA UNFAIR**  
) **COMPETITION LAW;**  
) 6) **VIOLATION OF THE**  
) **CALIFORNIA CUSTOMER**  
) **RECORDS ACT; and**  
) 7) **VIOLATION OF THE**  
) **CALIFORNIA CONSUMERS**  
) **LEGAL REMEDIES ACT**  
**JURY TRIAL DEMANDED**

1 Plaintiffs Wendy and Roy Duran (“Plaintiffs”), individually and on behalf of  
2 the classes defined below, bring this Class Action Complaint (“Complaint”) against  
3 Equifax, Inc. (“Equifax”), based upon personal knowledge with respect to  
4 themselves and on information and belief derived from, among other things,  
5 investigation of counsel and review of public documents as to all other matters, and  
6 allege as follows:

7 **I. INTRODUCTION**

8 1. On September 7, 2017, Equifax announced a nationwide data breach  
9 affecting an estimated 143 million consumers (the “Data Breach”). According  
10 to Equifax’s press release and other public statements, unauthorized parties  
11 accessed consumers’ sensitive, personal information maintained by Equifax by  
12 exploiting a website application vulnerability. Equifax claims that based on its  
13 investigation, the unauthorized access occurred from mid-May through July  
14 2017. The information included names, addresses, Social Security numbers,  
15 dates of birth, and, in some instances, driver’s license numbers. Equifax also  
16 admitted that credit card numbers for approximately 209,000 consumers, and  
17 certain dispute documents with personal identifying information (“PII”) for  
18 approximately 182,000 consumers were accessed.

19 2. The Data Breach occurred because Equifax failed to implement  
20 adequate security measures to safeguard Plaintiffs’ and other consumers’ PII  
21 and willfully ignored known weaknesses in its data security, including prior  
22 hacks into its information systems. Unauthorized parties routinely attempt to  
23 gain access to and steal personal information from networks and information  
24 systems—especially from entities such as Equifax, which are known to possess  
25 a large number of individuals’ valuable personal and financial information.

26 3. Armed with the personal information obtained in the Data Breach,  
27 identity thieves can commit a variety of crimes that harm victims of the Data  
28 Breach. For instance, they can take out loans, mortgage property, and open

1 financial accounts and credit cards in a victim's name; use a victim's  
2 information to obtain government benefits or file fraudulent returns to obtain a  
3 tax refund; obtain a driver's license or identification card in a victim's name;  
4 gain employment in a victim's name; obtain medical services in a victim's  
5 name; or give false information to police during an arrest. Hackers also  
6 routinely sell individuals' PII to other criminals who intend to misuse the  
7 information.

8       4. As a result of Equifax's willful failure to prevent the Data Breach,  
9 Plaintiffs and class members have been exposed to fraud, identity theft, and  
10 financial harm, as detailed below, and to a heightened, imminent risk of such  
11 harm in the future. Plaintiffs and class members have to monitor their financial  
12 accounts and credit histories more closely and frequently to guard against  
13 identity theft. Class members also have incurred, and will continue to incur,  
14 additional out-of-pocket costs for obtaining credit reports, credit freezes, credit  
15 monitoring services, and other protective measures in order to detect, protect,  
16 and repair the Data Breach's impact on their PII for the remainder of their lives.  
17 Plaintiffs have already spent time addressing the Data Breach and anticipate  
18 spending considerable time and money for the rest of their lives in order to  
19 detect and respond to the impact of the Data Breach.

20       5. There is a strong likelihood that class members already have or will  
21 become victims of identity fraud given the breadth of their PII that is now  
22 publicly available. Javelin Strategy & Research reported in its 2014 Identity  
23 Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud."  
24 In fact, "[i]n 2013, one in three consumers who received notification of a data  
25 breach became a victim of fraud." Javelin also found increased instances of  
26 fraud other than credit card fraud, including "compromised lines of credit,  
27 internet accounts (e.g., eBay, Amazon) and email payment accounts such as  
28 PayPal."

1           6.       Plaintiffs bring this action to remedy these harms on behalf of  
2 themselves and all similarly situated individuals whose PII was accessed during  
3 the Data Breach. Plaintiffs seek the following remedies, among others: statutory  
4 damages under the Fair Credit Reporting Act (“FCRA”) and state consumer  
5 protection statutes, reimbursement of out-of-pocket losses, other compensatory  
6 damages, further credit monitoring services with accompanying identity theft  
7 insurance beyond Equifax’s current one-year offer, and injunctive relief  
8 including an order requiring Equifax to implement improved data security  
9 measures.

## 10   **II. JURISDICTION AND VENUE**

11           7.       This Court has federal question jurisdiction under 28 U.S.C. § 1331  
12 because Plaintiffs are bringing claims under the FCRA, 15 U.S.C. §§ 1681e, *et seq.*

13           8.       This Court also has diversity jurisdiction under the Class Action  
14 Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more  
15 than 100 class members, the amount in controversy exceeds \$5 million exclusive of  
16 interest and costs, and many members of the proposed classes are citizens of states  
17 different from Equifax.

18           9.       Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because  
19 Equifax regularly transacts business here, and Plaintiffs and some of the class  
20 members reside in this District. In addition, the events giving rise to Plaintiffs’  
21 causes of action arose, in part, in this District.

## 22   **III. PARTIES**

### 23           **A. Plaintiffs**

24           10.       Plaintiffs are residents of Fullerton, California and were California  
25 residents during the period of the Data Breach. Plaintiffs previously provided their  
26 PII to Equifax and/or one of Equifax’s many clients including, but not limited to,  
27 their names, Social Security numbers and dates of birth. Plaintiffs are victims of  
28 the Data Breach. After Plaintiffs received notice of the Data Breach and were

1 informed that they were impacted by the Data Breach, Plaintiffs spent several hours  
2 addressing the potential impact of the Data Breach, and are taking action to protect  
3 their PII from further compromise. Plaintiffs have also spent time and effort  
4 monitoring their financial accounts, and anticipate spending more time and effort  
5 monitoring their financial accounts in the future as a result of the Data Breach.

6 **B. Defendants**

7 11. Equifax is a Delaware corporation with its principal place of business  
8 located at 1550 Peachtree Street NE, Atlanta, Georgia 30309. Equifax may be  
9 served through its registered agent, Shawn Baldwin, at its principal office address  
10 identified above.

11 12. The true names and/or capacities, whether individual, corporate,  
12 associate or otherwise, of defendants DOES 1 through 10 inclusive, and each of  
13 them, are unknown. Plaintiffs therefore sue these defendants by fictitious names.  
14 Plaintiffs are informed and believes, and upon such information and belief hereby  
15 alleges, that each of the defendants and fictitiously named herein as a DOE is  
16 legally responsible, negligently or in some other manner, for the events and  
17 happenings hereinafter referred to and proximately caused the damages to Plaintiffs  
18 and class members as hereinafter alleged. Plaintiffs will seek leave of court to  
19 amend this Complaint to insert the true names and/or capacities of such fictitiously  
20 named defendants when the same have been ascertained.

21 13. At all times herein mentioned, defendants, and each of them, were an  
22 agent or joint venturer of each of the other defendants, and in doing the acts alleged  
23 herein, were acting with the course and scope of such agency. Each defendant had  
24 actual and/or constructive knowledge of the acts of each of the other defendants,  
25 and ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of  
26 each co-defendant, and/or retained the benefits of said wrongful acts.

27 14. Defendants, and each of them, aided and abetted, encouraged and  
28 rendered substantial assistance to the other defendants in breaching their obligations

1 to Plaintiffs and the members of the proposed classes, as alleged herein. In taking  
2 action, as particularized herein, to aid and abet and substantially assist the  
3 commissions of these wrongful acts and other wrongdoings complained of, each of  
4 the defendants acted with an awareness of his/her/its primary wrongdoing and  
5 realized that his/her/its conduct would substantially assist the accomplishment of  
6 the wrongful conduct, wrongful goals, and wrongdoing.

7 15. Equifax is one of the major credit reporting bureaus in the United  
8 States. As a credit bureau service, Equifax is engaged in a number of credit-related  
9 services for individuals, businesses, and compliance with government regulations.  
10 Specifically, Equifax provides business services to the automotive,  
11 communications, utilities and digital media, education, financial services,  
12 healthcare, insurance, mortgage, restaurant, retail and wholesale trade, staffing, and  
13 transportation and distribution industries.<sup>1</sup> Equifax markets and sells many  
14 products to consumers and businesses, including Consumer Reports, which  
15 provides “access to current personally identifiable information for over 210 million  
16 consumers.”<sup>2</sup> Equifax’s Consumer Reports also includes “tradelines on over 1.8  
17 billion trades updated monthly” and “600 million unique, annual inquiries.”  
18 Equifax’s Consumer Reports provides “access to the consumer’s name, current  
19 address, address, previous former addresses, birth date, former names and Social  
20 Security number.” Equifax’s Consumer Reports is a product designed to “increase  
21 revenue”:<sup>3</sup>

---

24 <sup>1</sup> See *Equifax’s Business Industries*, EQUIFAX,  
25 <http://www.equifax.com/business/> (last visited Sept. 8, 2017).

26 <sup>2</sup> See *Equifax’s Consumer Reports Product Overview*, EQUIFAX,  
<http://www.equifax.com/business/consumer-reports> (last visited Sept. 8, 2017).

27 <sup>3</sup> See *Equifax’s Consumer Reports Product Sheet*, EQUIFAX,  
28 [http://www.equifax.com/assets/USCIS/efx-00198\\_consumer\\_reports.pdf](http://www.equifax.com/assets/USCIS/efx-00198_consumer_reports.pdf) (last  
visited Sept. 8, 2017).

1 **Make effective decisions that increase revenue**

2 Trust Equifax Consumer Reports to deliver the powerful combination of predictive consumer credit data and proven expertise backed by unmatched  
3 industry leadership. Make faster decisions with the competitive advantage of data speed and system integrity. Strengthen predictive ability, mitigate  
4 risk, manage acquisition costs and increase revenue with proven decisioning insight from Equifax Consumer Reports.

5 **IV. STATEMENT OF FACTS**

6 **A. The Data Breach Compromised the PII of 143 Million Consumers**

7 16. On September 7, 2017, Equifax announced that its systems had been  
8 breached and that the Data Breach affected approximately 143 million consumers.  
9 According to Equifax's website regarding the Data Breach, unauthorized users  
10 acquired the PII of approximately 143 million consumers from certain files  
11 maintained and stored by Equifax. The PII included names, addresses, Social  
12 Security numbers, dates of birth, and, in some instances, driver's license numbers,  
13 and other personal information:

14 Equifax today announced a cybersecurity incident  
15 potentially impacting approximately **143 million U.S.**  
16 **consumers**. Criminals exploited a U.S. website  
17 application vulnerability to gain access to certain files.  
18 Based on the company's investigation, the unauthorized  
19 access occurred from mid-May through July 2017.

19 ...  
20 The information accessed primarily includes **names,**  
21 **Social Security numbers, birth dates, addresses and, in**  
22 **some instances, driver's license numbers**. In addition,  
23 **credit card numbers for approximately 209,000**  
24 **consumers, and certain dispute documents with**  
25 **personal identifying information for approximately**  
26 **182,000 consumers**, were accessed.<sup>4</sup>

24 17. On its website, Equifax admits learning of the Data Breach on July 29,  
25 2017, but only began notifying consumers through a press release and generic  
26

27 \_\_\_\_\_  
28 <sup>4</sup> See *Cybersecurity Incident & Important Consumer Information*, EQUIFAX,  
<https://www.equifaxsecurity2017.com/> (last visited Sept. 8, 2017).



1 website at <https://www.equifaxsecurity2017.com> on September 7, 2017, almost  
2 four months after the Data Breach began.<sup>5</sup>

3 18. Instead of immediately notifying consumers when it discovered the  
4 Data Breach, Equifax executives sold at least \$1.8 million worth of shares before  
5 the public disclosure of the breach. It has been reported that its Chief Financial  
6 Officer John Gamble sold shares worth \$946,374, its president of U.S. information  
7 solutions, Joseph Loughran, exercised options to dispose of stock worth \$584,099,  
8 and its president of workforce solutions, Rodolfo Ploder, sold \$250,458 of stock on  
9 August 2, 2017.<sup>6</sup>

10 19. In response to the questions of “Why am I learning about this incident  
11 through the media?” and “Why didn’t Equifax notify me directly?”, Equifax states  
12 that it “issued a national press release in order to notify U.S. consumers of this  
13 incident and has established a website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), where U.S.  
14 consumers can receive further information.”<sup>7</sup>

15 20. Despite the fact that Equifax has the names and addresses for the 143  
16 million U.S. Data Breach victims, Equifax has not provided direct mail notices to  
17 them; rather, Equifax states that it will only provide direct mail notice to the  
18 209,000 consumers whose credit card numbers and 182,000 consumers whose  
19 dispute documents with PII were impacted.<sup>8</sup>

20 21. On its website, Equifax admits the unauthorized disclosure of consumer  
21 data and warned consumers of the consequences of the Data Breach:  
22

---

23 <sup>5</sup> See *Cybersecurity Incident & Important Consumer Information*, EQUIFAX,  
24 <https://www.equifaxsecurity2017.com/frequently-asked-questions/> (last visited Sept.  
25 8, 2017).

26 <sup>6</sup> See *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*,  
27 BLOOMBERG, [https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-  
28 executives-sold-stock-before-revealing-cyber-hack](https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack) (last visited Sept. 8, 2017).

<sup>7</sup> *Id.*

<sup>8</sup> See *Cybersecurity Incident & Important Consumer Information*, EQUIFAX,  
<https://www.equifaxsecurity2017.com/> (last visited Sept. 8, 2017).



1 We recommend that consumers be vigilant in reviewing  
2 their account statements and credit reports, and that they  
3 immediately report any unauthorized activity to their  
4 financial institutions. We also recommend that they  
5 monitor their personal information and visit the Federal  
6 Trade Commission's, website, [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), to  
7 obtain information about steps they can take to better  
8 protect against identity theft as well as information about  
9 fraud alerts and security freezes.<sup>9</sup>

10 22. On its Data Breach website, Equifax invites individuals to determine if  
11 their personal information may have been impacted by the Data Breach by  
12 providing their last name and the last six digits of their Social Security number. If  
13 an individual is determined to have been affected, Equifax provides them with a  
14 date to return to the website to enroll in Equifax's TrustedID Premier credit  
15 monitoring service. If an individual is determined to have not been affected,  
16 Equifax provides them with this information, but then still provides them with a  
17 link to enroll in (and pay for) Equifax's TrustedID Premier credit monitoring  
18 service.

19 **B. Equifax Promised to Protect its Customers' PII, but Maintained**  
20 **Inadequate Data Security**

21 23. Equifax is one of the major credit reporting bureaus in the United  
22 States. As a credit bureau service, Equifax is engaged in a number of credit-related  
23 services for individuals, businesses, and compliance with government regulations.  
24 Specifically, Equifax provides business services to the automotive,  
25 communications, utilities and digital media, education, financial services,  
26 healthcare, insurance, mortgage, restaurant, retail and wholesale trade, staffing, and  
27 transportation and distribution industries.<sup>10</sup> Equifax markets and sells many

28 <sup>9</sup> See *Cybersecurity Incident & Important Consumer Information*, EQUIFAX,  
<https://www.equifaxsecurity2017.com/frequently-asked-questions/> (last visited Sept.  
8, 2017).

<sup>10</sup> See *Equifax's Business Industries*, EQUIFAX,  
<http://www.equifax.com/business/> (last visited Sept. 8, 2017).

1 products to consumers and businesses, including Consumer Reports, which  
2 provides “access to current personally identifiable information for over 210 million  
3 consumers.”<sup>11</sup> Equifax’s Consumer Reports also includes “tradelines on over 1.8  
4 billion trades updated monthly” and “600 million unique, annual inquiries.”  
5 Equifax’s Consumer Reports provides “access to the consumer’s name, current  
6 address, address, previous former addresses, birth date, former names and Social  
7 Security number.”<sup>12</sup>

8 24. Prior to the Data Breach, Equifax promised its customers and everyone  
9 else whose PII it collects that it would reasonably protect their PII. Equifax’s  
10 privacy policy stated, in relevant part:

11 We have built our reputation on our commitment to  
12 deliver reliable information to our customers (both  
13 businesses and consumers) and to *protect the privacy  
14 and confidentiality of personal information about  
15 consumers*. We also protect the sensitive information we  
16 have about businesses. *Safeguarding the privacy and  
17 security of information, both online and offline, is a top  
18 priority for Equifax.*<sup>13</sup>

19 25. Equifax’s policy further stated:

20 We are committed to protecting the security of your  
21 information through procedures and technology designed  
22 for this purpose by taking these steps:

- 23 • We limit access to your personal information to  
24 employees having a reasonable need to access this  
25 information to provide products and services to you.  
26 Employees who misuse information are subject to

27 <sup>11</sup> See *Equifax’s Consumer Reports Product Overview*, EQUIFAX,  
28 <http://www.equifax.com/business/consumer-reports> (last visited Sept. 8, 2017).

<sup>12</sup> See *Equifax’s Consumer Reports Product Sheet*, EQUIFAX,  
[http://www.equifax.com/assets/USCIS/efx-00198\\_consumer\\_reports.pdf](http://www.equifax.com/assets/USCIS/efx-00198_consumer_reports.pdf) (last  
visited Sept. 8, 2017).

<sup>13</sup> See *Equifax’s Privacy Policy*, EQUIFAX, <http://www.equifax.com/privacy/>  
(last visited Sept. 8, 2017).

1 disciplinary action, including termination.

- 2
- 3 • We have reasonable physical, technical and
  - 4 procedural safeguards to help protect your personal
  - 5 information.
  - 6 • In areas that contain your personal information, we
  - 7 use secure socket layer (SSL) encryption to help
  - 8 protect this information while it is in transit between
  - 9 our servers and your computer.<sup>14</sup>

10 26. Plaintiffs and Class members disclosed their PII to Equifax in

11 connection with consumer transactions and Equifax compiled, maintained,

12 furnished, and made available Plaintiffs' and class members' PII. Equifax was

13 allowed to perform such services involving sensitive information only if it adhered

14 to the requirements of laws meant to protect the privacy of such information, such

15 as the FCRA and the Gramm-Leach-Bliley Act ("GLBA"). Equifax's maintenance,

16 use, and furnishing of such PII is and was intended to affect Plaintiffs and other

17 class members, and the harm caused by disclosure of that PII in the Data Breach

18 was entirely foreseeable to Equifax.

19 **C. Equifax Experienced Prior Data Breaches, but Nevertheless Failed**

20 **to Implement Appropriate Security**

21 27. Although Equifax claims to be a leader in data security and its privacy

22 policy promises to reasonably safeguard consumer data, Equifax's own data

23 security practices were inadequate. Equifax was well aware of this fact because it

24 had experienced multiple data breaches in recent years.

25 28. In March 2014, Equifax reported a data breach to the New Hampshire

26 Attorney General involving an IP address operator who was able to obtain Equifax

27 consumer credit reports using sufficient personal information to bypass Equifax's

28 <sup>14</sup> See *Equifax's Personal Credit Reports Privacy Policy*, EQUIFAX, <http://www.equifax.com/privacy/> (last visited Sept. 8, 2017).

1 identity verification process.<sup>15</sup>

2 29. In May 2016, Equifax's W-2 Express website suffered a data breach  
3 where an attacker was able to access, download and post the names, addresses,  
4 social security numbers and other personal information of over 430,000 Kroger  
5 employees. The attackers were able to access the W-2 data by merely entering  
6 Equifax's portal with an employee's default PIN code, which was the last four  
7 digits of the employee's Social Security number and their four-digit birth year.<sup>16</sup>

8 30. Independent security researchers have also found that Equifax's  
9 website is vulnerable. In 2016, a security researcher found a common vulnerability  
10 known as cross-site scripting (XSS) on the main Equifax website. Such XSS bugs  
11 allow attackers to send specially-crafted links to Equifax customers and, if the  
12 target clicks through and is logged into the site, their username and password can  
13 be revealed to the hacker.<sup>17</sup>

14 31. Researcher Kenneth White just recently discovered a link in the source  
15 code on the Equifax consumer sign-in page that pointed to Netscape, a web browser  
16 that was discontinued in 2008. Kevin Beaumont, a British security professional,  
17 found decade-old software in use, including IBM WebSphere, Apache Struts and  
18 Java, many of which are outdated and subject to well-known vulnerabilities.<sup>18</sup>

19  
20  
21  
22 <sup>15</sup> See *Letter from Troy G. Kubes, Vice President & Associate Group Counsel*  
23 *at Equifax Legal Department, to Attorney General Joseph Foster, MAR. 5, 2014,*  
24 [https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-](https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf)  
25 [20140305.pdf](https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf) (last visited Sept. 8, 2017).

26 <sup>16</sup> See *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY,  
27 <http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/>  
28 (last visited Sept. 8, 2017).

<sup>17</sup> See *A Brief History Of Equifax Security Fails*, FORBES,  
[https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-](https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#53a60715677c)  
history/#53a60715677c (last visited Sept. 8, 2017).

<sup>18</sup> *Id.*

1           **D.     The Data Breach has Exposed Plaintiffs and Other Consumers to**  
2           **Fraud, Identity Theft, Financial Harm, and a Heightened,**  
3           **Imminent Risk of Such Harm in the Future**

4           32.     Since identity thieves use the PII of other people to commit fraud or  
5 other crimes, Plaintiffs and other consumers whose information was exposed in the  
6 Data Breach are subject to an increased, concrete risk of identity theft. Javelin  
7 Strategy & Research, a research-based consulting firm that specializes in fraud and  
8 security in advising its clients, reported in its 2014 Identity Fraud Study that “[d]ata  
9 breaches are the greatest risk factor for identity fraud.” In fact, “[i]n 2013, one in  
10 three consumers who received notification of a data breach became a victim of  
11 fraud.” Javelin also found increased instances of fraud other than credit card fraud,  
12 including “compromised lines of credit, internet accounts (*e.g.*, eBay, Amazon) and  
13 email payment accounts such as PayPal.”<sup>19</sup>

14           33.     The exposure of Plaintiffs’ and class members’ Social Security  
15 numbers in particular poses serious problems. Criminals frequently use Social  
16 Security numbers to create false bank accounts, file fraudulent tax returns, and  
17 incur credit in the victim’s name. Neal O’Farrell, a security and identity theft  
18 expert for Credit Sesame calls a Social Security number “your secret sauce,” that is  
19 “as good as your DNA to hackers.”<sup>20</sup> Even where data breach victims obtain a new  
20 Social Security number, the Social Security Administration warns “that a new  
21 number probably will not solve all [] problems . . . and will not guarantee [] a fresh  
22  
23

24 \_\_\_\_\_  
25           <sup>19</sup> See [https://www.javelinstrategy.com/press-release/new-identity-fraud-](https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy)  
26 [victim-every-two-seconds-2013-according-latest-javelin-strategy](https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy) (last visited April  
14, 2016).

27           <sup>20</sup> Tips, How to Protect Your Kids From the Anthem Data Breach,” Kiplinger  
(Feb. 10, 2015), *available at*

28           [http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-](http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html)  
[your-kids-from-the-anthem-data-brea.html](http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html) (last visited April 14, 2016).

1 start.”<sup>21</sup> In fact, “[f]or some victims of identity theft, a new number actually creates  
2 new problems.” One of those new problems is that a new Social Security number  
3 will have a completely blank credit history, making it difficult to get credit for a  
4 few years unless it is linked to the old compromised number.

5 34. As a result of the compromising of their personal information,  
6 Plaintiffs and class members will face an increased risk of experiencing the  
7 following injuries:

- 8 • money and time expended to prevent, detect, contest, and repair  
9 identity theft, fraud, and/or other unauthorized uses of personal  
10 information;
- 11 • money and time lost as a result of fraudulent access to and use of their  
12 financial accounts;
- 13 • loss of use of and access to their financial accounts and/or credit;
- 14 • impairment of their credit scores, ability to borrow, and/or ability to  
15 obtain credit;
- 16 • lowered credit scores resulting from credit inquiries following  
17 fraudulent activities;
- 18 • costs and lost time obtaining credit reports in order to monitor their  
19 credit records;
- 20 • money, including fees charged in some states, and time spent placing  
21 fraud alerts and security freezes on their credit records;
- 22 • money and time expended to avail themselves of assets and/or credit  
23 frozen or flagged due to misuse;
- 24 • costs of credit monitoring that is more robust than the services being  
25 offered by Equifax;
- 26

---

27 <sup>21</sup> Social Security Administration, Identity Theft and Your Social Security  
28 Number, pp. 7-8, *available at* <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last  
visited Mar. 10, 2016)

- 1 • anticipated future costs from the purchase of credit monitoring and/or
- 2 identity theft protection services once the temporary services being
- 3 offered by Equifax expire;
- 4 • costs and lost time from dealing with administrative consequences of
- 5 the Data Breach, including by identifying, disputing, and seeking
- 6 reimbursement for fraudulent activity, canceling compromised financial
- 7 accounts and associated payment cards, and investigating options for
- 8 credit monitoring and identity theft protection services;
- 9 • money and time expended to ameliorate the consequences of the filing
- 10 of fraudulent tax returns;
- 11 • lost opportunity costs and loss of productivity from efforts to mitigate
- 12 and address the adverse effects of the Data Breach including, but not
- 13 limited to, efforts to research how to prevent, detect, contest, and
- 14 recover from misuse of their personal information;
- 15 • loss of the opportunity to control how their personal information is
- 16 used; and
- 17 • continuing risks to their personal information, which remains subject to
- 18 further harmful exposure and theft as long as Equifax fails to undertake
- 19 appropriate, legally required steps to protect the personal information in
- 20 its possession.

21 35. The risks that Plaintiffs and Class members bear as a result of the Data  
22 Breach cannot be mitigated by the credit monitoring Equifax has offered to affected  
23 consumers because it can only help detect, but will not prevent, the fraudulent use  
24 of Plaintiffs' and class members' PII. Instead, Plaintiffs and class members will  
25 need to spend time and money to protect themselves. For instance, credit reporting  
26 agencies impose fees for credit freezes in certain states. In addition, while credit  
27 reporting agencies offer consumers one free credit report per year, consumers who  
28 request more than one credit report per year from the same credit reporting agency



1 (such as Equifax) must pay a fee for the additional report. Such fees constitute out-  
2 of-pocket costs to Plaintiffs and class members.

3 36. The risks borne by affected consumers are not hypothetical: Equifax  
4 has admitted that class members' personal information was disclosed and  
5 downloaded in the Data Breach, has admitted the risks of identity theft, and has  
6 encouraged consumers to vigilantly monitor their accounts.

7 **E. Equifax was Required to Investigate and Provide Timely and**  
8 **Adequate Notification of the Data Breach under Federal**  
9 **Regulations**

10 37. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial  
11 institutions" "an affirmative and continuing obligation to respect the privacy of its  
12 customers and to protect the security and confidentiality of those customers'  
13 nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation,  
14 financial institutions must satisfy certain standards relating to administrative,  
15 technical, and physical safeguards:

16 (1) to *insure the security and confidentiality of customer*  
17 *records and information;*

18 (2) to *protect against any anticipated threats or hazards to*  
19 *the security or integrity of such records;* and

20 (3) to *protect against unauthorized access to or use of such*  
21 *records* or information which could result in substantial  
22 harm or inconvenience to any customer. 15 U.S.C. §  
23 6801(b) (emphasis added).

24 38. In order to satisfy their obligations under the GLBA, financial  
25 institutions must "develop, implement, and maintain a comprehensive information  
26 security program that is [1] written in one or more readily accessible parts and [2]  
27 contains administrative, technical, and physical safeguards that are appropriate to  
28 [their] size and complexity, the nature and scope of [their] activities, and the

1 sensitivity of any customer information at issue.” 16 C.F.R. § 314.4. “In order to  
2 develop, implement, and maintain [their] information security program, [financial  
3 institutions] shall:

4 (a) Designate an employee or employees to coordinate  
5 [their] information security program.

6 (b) ***Identify reasonably foreseeable internal and external***  
7 ***risks to the security, confidentiality, and integrity of***  
8 ***customer information*** that could result in the  
9 unauthorized disclosure, misuse, alteration, destruction  
10 or other compromise of such information, and assess the  
11 sufficiency of any safeguards in place to control these  
12 risks. At a minimum, such a risk assessment should  
include consideration of risks in each relevant area of  
[their] operations, including:

13 (1) Employee training and management;

14 (2) Information systems, including network and software  
15 design, as well as information processing, storage,  
16 transmission and disposal; and

17 (3) Detecting, preventing and responding to attacks,  
18 intrusions, or other systems failures.

19 (c) ***Design and implement information safeguards to***  
20 ***control the risks [they] identify through risk***  
21 ***assessment***, and regularly test or otherwise monitor the  
22 effectiveness of the safeguards’ key controls, systems,  
and procedures.

23 (d) Oversee service providers, by:

24 (1) Taking reasonable steps to select and retain service  
25 providers that are capable of maintaining appropriate  
26 safeguards for the customer information at issue; and

27 (2) Requiring [their] service providers by contract to  
28 implement and maintain such safeguards.

1 (e) *Evaluate and adjust [their] information security*  
2 *program in light of the results* of the testing and  
3 monitoring required by paragraph (c) of this section; any  
4 material changes to [their] operations or business  
5 arrangements; or any other circumstances that [they]  
know or have reason to know may have a material  
impact on [their] information security program.”

6 *Id.*

7 39. In addition, under the Interagency Guidelines Establishing Information  
8 Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an  
9 affirmative duty to “develop and implement a risk-based response program to  
10 address incidents of unauthorized access to customer information in customer  
11 information systems.” *See id.* “At a *minimum*, an institution’s response program  
12 should contain procedures for the following:

- 13 a. Assessing the nature and scope of an incident, and  
14 identifying what customer information systems and types  
15 of customer information have been accessed or misused;
- 16 b. Notifying its primary Federal regulator as soon as  
17 possible when the institution becomes aware of an  
18 incident involving unauthorized access to or use of  
sensitive customer information, as defined below;
- 19 c. Consistent with the Agencies’ Suspicious Activity Report  
20 (“SAR”) regulations, notifying appropriate law  
21 enforcement authorities, in addition to filing a timely  
22 SAR in situations involving Federal criminal violations  
23 requiring immediate attention, such as when a reportable  
violation is ongoing;
- 24 d. Taking appropriate steps to contain and control the  
25 incident to prevent further unauthorized access to or use  
26 of customer information, for example, by monitoring,  
27 freezing, or closing affected accounts, while preserving  
records and other evidence; and
- 28 e. Notifying customers when warranted.

1 *Id.* (emphasis added).

2 40. Further, “[w]hen a financial institution becomes aware of an incident of  
3 unauthorized access to sensitive customer information, the institution should  
4 conduct a reasonable investigation to promptly determine the likelihood that the  
5 information has been or will be misused. If the institution determines that misuse  
6 of its information about a customer has occurred or is reasonably possible, it should  
7 notify the affected customer as soon as possible.” *See id.*

8 41. Credit bureaus are “financial institutions” for purposes of the GLBA,  
9 and are therefore subject to its provisions. *See TranUnion LLC v. F.T.C.*, 295 F.3d  
10 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve  
11 Board, *Bank Holding Companies and Change in Bank Control*, “credit bureau  
12 services”<sup>22</sup> are “so closely related to banking or managing or controlling banks as to  
13 be a proper incident thereto.” Since Equifax is a credit bureau and performs credit  
14 bureau services, it qualifies as a financial institution for purposes of the GLBA.

15 42. “Nonpublic personal information,” includes PII (such as the PII  
16 compromised during the Data Breach) for purposes of the GLBA. Likewise,  
17 “sensitive customer information” includes PII for purposes of the Interagency  
18 Guidelines Establishing Information Security Standards.

19 43. Upon information and belief, Equifax failed to “develop, implement,  
20 and maintain a comprehensive information security program” with “administrative,  
21 technical, and physical safeguards” that were “appropriate to [its] size and  
22 complexity, the nature and scope of [its] activities, and the sensitivity of any  
23 customer information at issue.” This includes, but is not limited to, (a) Equifax’s  
24 failure to implement and maintain adequate data security practices to safeguard  
25 class members’ PII; (b) failing to detect the Data Breach in a timely manner; and

26 \_\_\_\_\_  
27 <sup>22</sup> Credit bureau services include “[m]aintaining information related to the  
28 credit history of consumers and providing the information to a credit grantor who is  
considering a borrower’s application for credit or who has extended credit to the  
borrower.” *See* 12 C.F.R. § 225.28.

1 (c) failing to disclose that its data security practices were inadequate to safeguard  
2 class members' PII.

3 44. Upon information and belief, Equifax also failed to “develop and  
4 implement a risk-based response program to address incidents of unauthorized  
5 access to customer information in customer information systems” as mandated by  
6 the GLBA. This includes, but is not limited to, Equifax’s failure to notify  
7 appropriate regulatory agencies, law enforcement, and the affected individuals  
8 themselves of the Data Breach in a timely and adequate manner.

9 45. Upon information and belief, Equifax also failed to notify affected  
10 customers as soon as possible after it became aware of unauthorized access to  
11 sensitive customer information.

## 12 V. CLASS ALLEGATIONS

13 46. Plaintiffs bring all claims as class claims under Federal Rule of Civil  
14 Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

### 15 A. Nationwide Class

16 47. Plaintiffs bring their FCRA, negligence, and negligence per se claims  
17 (Counts I-IV) on behalf of a proposed nationwide class (“Nationwide Class”),  
18 defined as follows:

19 *All natural persons and entities in the United States whose*  
20 *personally identifiable information was acquired by unauthorized*  
21 *persons in the data breach announced by Equifax in September*  
22 *2017.*

### 23 B. Statewide Classes

24 48. Plaintiffs bring their state consumer protection statute and data breach  
25 notification claims (Counts V through VII) on behalf of a separate California  
26 Subclass.

1           49. Plaintiffs also bring their negligence and negligence per se claims  
2 (counts III and IV) separately on behalf of the California Subclass, in the alternative  
3 to bringing those claims on behalf of the Nationwide Class.

4           50. Except where otherwise noted, “Class Members” shall refer to members  
5 of the Nationwide Class and California Subclass, collectively.

6           51. Excluded from the Nationwide Class and California Subclass are  
7 defendants and their current employees, as well as the Court and its personnel  
8 presiding over this action.

9           52. The Nationwide and California Subclass meet the requirements of  
10 Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the  
11 reasons set forth in Paragraphs 53-62:

12           53. **Numerosity:** The Nationwide and California Subclass are so numerous  
13 that joinder of all members is impracticable. According to Equifax, the Nationwide  
14 Class includes approximately 143 million individuals whose PII was acquired  
15 during the Data Breach. On information and belief, Plaintiffs allege that there are  
16 millions of individuals in the California Subclass. The parties will be able to  
17 identify each member of the Nationwide Class and California Subclass after  
18 Equifax’s document production and/or related discovery.

19           54. **Commonality:** There are numerous questions of law and fact common  
20 to Plaintiffs and the Nationwide and California Subclass including, but not limited  
21 to, the following:

- 22           • whether Equifax engaged in the wrongful conduct alleged herein;
- 23           • whether Equifax owed a duty to Plaintiffs and Class Members to  
24           adequately protect their PII;
- 25           • whether Equifax breached its duties to protect the personal information  
26           of Plaintiffs and Class Members;
- 27           • whether Equifax knew or should have known that its data security  
28           systems and processes were vulnerable to attack;

- 1 • whether Plaintiffs and Class Members suffered legally cognizable
- 2 damages as a result of Equifax's conduct, including increased risk of
- 3 identity theft and loss of value of PII;
- 4 • whether Equifax violated the FCRA; and
- 5 • whether Plaintiffs and Class Members are entitled to equitable relief
- 6 including injunctive relief.

7 55. **Typicality:** Plaintiffs' claims are typical of the claims of the  
8 Nationwide Class, and Plaintiffs' claims are typical of the claims of the California  
9 Subclass. Plaintiffs, like all proposed Class Members, had their PII compromised in  
10 the Data Breach.

11 56. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of  
12 the Nationwide Class and California Subclass. Plaintiffs have no interests that are  
13 adverse to, or in conflict with, the Class Members. There are no claims or defenses  
14 that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced  
15 in class action and complex litigation, including data breach litigation, that have  
16 sufficient resources to prosecute this action vigorously.

17 57. **Predominance:** The proposed action meets the requirements of Federal  
18 Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the  
19 Nationwide Class and California Subclass predominate over any questions which  
20 may affect only individual Class members in any of the proposed classes, including  
21 those listed in paragraph 40, *supra*.

22 58. **Superiority:** The proposed action also meets the requirements of  
23 Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other  
24 available methods for the fair and efficient adjudication of the controversy. Class  
25 treatment of common questions is superior to multiple individual actions or  
26 piecemeal litigation, avoids inconsistent decisions, presents far fewer management  
27 difficulties, conserves judicial resources and the parties' resources, and protects the  
28 rights of the Class Members.



1 59. Absent a class action, the majority of Class Members would find the  
2 cost of litigating their claims prohibitively high and would have no effective  
3 remedy.

4 60. **Risks of Prosecuting Separate Actions:** Plaintiffs' claims also meet  
5 the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution  
6 of separate actions by individual Class Members would create a risk of inconsistent  
7 or varying adjudications that would establish incompatible standards for Equifax.  
8 Equifax continues to maintain the PII of the Class Members and other individuals,  
9 and varying adjudications could establish incompatible standards with respect to:  
10 Equifax's duty to protect individuals' PII; whether Equifax's ongoing conduct  
11 violates the FCRA and other claims alleged herein; and whether the injuries  
12 suffered by Class Members are legally cognizable, among others. Prosecution of  
13 separate actions by individual Class Members would also create a risk of individual  
14 adjudications that would be dispositive of the interests of other Class Members not  
15 parties to the individual adjudications, or substantially impair or impede the ability  
16 of Class Members to protect their interests.

17 61. **Injunctive Relief:** In addition, Equifax has acted and/or refused to act  
18 on grounds that apply generally to the Nationwide and California Subclass, making  
19 injunctive and/or declaratory relief appropriate with respect to the classes under  
20 Federal Rule of Civil Procedure 23(b)(2). Equifax continues to (1) maintain the PII  
21 of Class Members, (2) fail to adequately protect their PII, and (3) violate their rights  
22 under the FCRA and other claims alleged herein.

23 62. **Certification of Particular Issues:** In the alternative, the Nationwide  
24 Class and California Subclass may be maintained as class actions with respect to  
25 particular issues, in accordance with Fed. R. Civ. P. 23(c)(4):

26 **VI. CAUSES OF ACTION**

27 **COUNT I**

28 **WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT**

**(On Behalf of the Nationwide Class)**

1  
2 63. Plaintiffs incorporate by reference all paragraphs above as if fully  
3 set forth herein.

4 64. As individuals, Plaintiffs and Class Members are consumers entitled  
5 to the protections of the FCRA. 15 U.S.C. § 1681a(c).

6 65. Under the FCRA, a “consumer reporting agency” is defined as “any  
7 person which, for monetary fees, dues, or on a cooperative nonprofit basis,  
8 regularly engages in whole or in part in the practice of assembling or evaluating  
9 consumer credit information or other information on consumers for the purpose  
10 of furnishing consumer reports to third parties . . . .” 15 U.S.C. § 1681a(f).

11 66. Equifax is a consumer reporting agency under the FCRA because for  
12 monetary fees, it regularly engages in the practice of assembling or evaluating  
13 consumer credit information or other information on consumers for the purpose  
14 of furnishing consumer reports to third parties.

15 67. As a consumer reporting agency, the FCRA requires Equifax to  
16 “maintain reasonable procedures designed to . . . limit the furnishing of  
17 consumer reports to the purposes listed under section 1681b of this title.” 15  
18 U.S.C. § 1681e(a).

19 68. Under the FCRA, a “consumer report” is defined as “any written,  
20 oral, or other communication of any information by a consumer reporting  
21 agency bearing on a consumer’s credit worthiness, credit standing, credit  
22 capacity, character, general reputation, personal characteristics, or mode of  
23 living which is used or expected to be used or collected in whole or in part for  
24 the purpose of serving as a factor in establishing the consumer’s eligibility for -  
25 - (A) credit . . . to be used primarily for personal, family, or household  
26 purposes; . . . or (C) any other purpose authorized under section 1681b of this  
27 title.” 15 U.S.C. § 1681a(d)(1).

28 69. The compromised data was a consumer report under the FCRA

1 because it was a communication of information bearing on Class members’  
2 credit worthiness, credit standing, credit capacity, character, general reputation,  
3 personal characteristics, or mode of living used, or expected to be used or  
4 collected in whole or in part, for the purpose of serving as a factor in  
5 establishing the Class members’ eligibility for credit.

6 70. As a consumer reporting agency, Equifax may only furnish a  
7 consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b,  
8 “and no other.” 15 U.S.C. § 1681b(a). None of the purposes listed under 15  
9 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to  
10 unauthorized or unknown entities, or computer hackers such as those who  
11 accessed the Nationwide Class members’ PII. Equifax violated § 1681b by  
12 furnishing consumer reports to unauthorized or unknown entities or computer  
13 hackers, as detailed above.

14 71. Equifax furnished the Nationwide Class members’ consumer reports  
15 by disclosing their consumer reports to unauthorized entities and computer  
16 hackers; allowing unauthorized entities and computer hackers to access their  
17 consumer reports; knowingly and/or recklessly failing to take security measures  
18 that would prevent unauthorized entities or computer hackers from accessing  
19 their consumer reports; and/or failing to take reasonable security measures that  
20 would prevent unauthorized entities or computer hackers from accessing their  
21 consumer reports.

22 72. The Federal Trade Commission (“FTC”) has pursued enforcement  
23 actions against consumer reporting agencies under the FCRA for failing “take  
24 adequate measures to fulfill their obligations to protect information contained in  
25 consumer reports, as required by the” FCRA, in connection with data breaches.

26 73. Equifax willfully violated § 1681b and § 1681e(a) by providing  
27 impermissible access to consumer reports and by failing to maintain reasonable  
28 procedures designed to limit the furnishing of consumer reports to the purposes

1 outlined under section 1681b of the FCRA. The willful nature of Equifax’s  
2 violations is supported by, among other things, former employees’ admissions  
3 that Equifax’s data security practices have deteriorated in recent years, and  
4 Equifax’s numerous other data breaches in the past. Further, Equifax touts  
5 itself as an industry leader in breach prevention; thus, Equifax was well aware  
6 of the importance of the measures organizations should take to prevent data  
7 breaches, and willingly failed to take them.

8       74. Equifax also acted willfully because it knew or should have known  
9 about its legal obligations regarding data security and data breaches under the  
10 FCRA. These obligations are well established in the plain language of the  
11 FCRA and in the promulgations of the Federal Trade Commission. See, e.g., 55  
12 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit  
13 Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E.  
14 Equifax obtained or had available these and other substantial written materials  
15 that apprised them of their duties under the FCRA. Any reasonable consumer  
16 reporting agency knows or should know about these requirements. Despite  
17 knowing of these legal obligations, Equifax acted consciously in breaching  
18 known duties regarding data security and data breaches and depriving Plaintiffs  
19 and other members of the classes of their rights under the FCRA.

20       75. Equifax’s willful and/or reckless conduct provided a means for  
21 unauthorized intruders to obtain and misuse Plaintiffs’ and Nationwide Class  
22 members’ personal information for no permissible purposes under the FCRA.

23       76. Plaintiffs and the Nationwide Class Members have been damaged by  
24 Equifax’s willful failure to comply with the FCRA. Therefore, Plaintiffs and  
25 each of the Nationwide Class members are entitled to recover “any actual  
26 damages sustained by the consumer . . . or damages of not less than \$100 and  
27 not more than \$1,000.” 15 U.S.C. § 1681n(a)(1)(A).

28       77. Plaintiffs and the Nationwide Class members are also entitled to

1 punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C.  
2 § 1681n(a)(2), (3).

3 **COUNT I**

4 **NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**  
5 **(On Behalf of the Nationwide Class)**

6 78. Plaintiffs incorporate by reference all paragraphs above as if fully set  
7 forth here.

8 79. Equifax was negligent in failing to maintain reasonable procedures  
9 designed to limit the furnishing of consumer reports to the purposes outlined under  
10 section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable  
11 procedures is supported by, among other things, former employees' admissions that  
12 Equifax's data security practices have deteriorated in recent years, and Equifax's  
13 numerous other data breaches in the past. Further, as an enterprise claiming to be  
14 an industry leader in data breach prevention, Equifax was well aware of the  
15 importance of the measures organizations should take to prevent data breaches, yet  
16 failed to take them.

17 80. Equifax's negligent conduct provided a means for unauthorized  
18 intruders to obtain Plaintiffs' and the Nationwide Class members' PII and  
19 consumer reports for no permissible purposes under the FCRA.

20 81. Plaintiffs and the Nationwide Class members have been damaged by  
21 Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and  
22 each of the Nationwide Class members are entitled to recover "any actual damages  
23 sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

24 82. Plaintiffs and the Nationwide Class members are also entitled to  
25 recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. §  
26 1681o(a)(2).

27 **COUNT II**

28 **NEGLIGENCE**

**(On Behalf of the Nationwide Class and California Subclass)**

1  
2 83. Plaintiffs incorporate by reference all paragraphs above as if fully set  
3 forth here.

4 84. Equifax owed a duty to Plaintiffs and Class Members, arising from the  
5 sensitivity of the information and the foreseeability of its data safety shortcomings  
6 resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive  
7 personal information. This duty included, among other things, designing,  
8 maintaining, monitoring, and testing Equifax's security systems, protocols, and  
9 practices to ensure that Class Members' information adequately secured from  
10 unauthorized access.

11 85. Equifax's privacy policy acknowledged Equifax's duty to adequately  
12 protect Class Members' PII.

13 86. Equifax owed a duty to Class Members to implement current and  
14 available technology that would prevent foreseeable data breaches, such as this one.

15 87. Equifax owed a duty to Class Members to implement intrusion  
16 detection processes that would detect a data breach in a timely manner.

17 88. Equifax also had a duty to delete any PII that was no longer needed to  
18 serve client needs.

19 89. Equifax owed a duty to disclose the material fact that its data security  
20 practices were inadequate to safeguard Class Members' PII.

21 90. Equifax also had independent duties under Plaintiffs' and Class  
22 Members' state laws that required Equifax to reasonably safeguard Plaintiffs' and  
23 Class Members' PII and promptly notify them about the Data Breach.

24 91. Equifax had a special relationship with Plaintiffs and Class Members  
25 from being entrusted with their PII, which provided an independent duty of care.  
26 Plaintiffs' and other Class Members' willingness to entrust Equifax with their PII  
27 was predicated on the understanding that Equifax would take adequate security  
28 precautions. Moreover, Equifax had the ability to protect its systems and the PII it

1 stored on them from attack.

2 92. Equifax's role to utilize and purportedly safeguard Plaintiffs' and Class  
3 Members' PII presents unique circumstances requiring a reallocation of risk.

4 93. Equifax breached its duties by, among other things: (a) failing to  
5 implement and maintain adequate data security practices to safeguard Class  
6 Members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing  
7 to disclose that Equifax's data security practices were inadequate to safeguard  
8 Class Members' PII; and (d) failing to provided adequate and timely notice of the  
9 Data Breach.

10 94. But for Equifax's breach of its duties, Class Members' PII would not  
11 have been accessed by unauthorized individuals.

12 95. Plaintiffs and Class Members were foreseeable victims of Equifax's  
13 inadequate data security practices. Equifax knew or should have known that a  
14 breach of its data security systems would cause damages to Class Members.

15 96. Equifax's negligent conduct provided a means for unauthorized  
16 intruders to obtain Plaintiffs' and the Nationwide Class Members' PII and  
17 consumer reports for no permissible purposes under the FCRA.

18 97. As a result of Equifax's willful failure to prevent the Data Breach,  
19 Plaintiffs and Class Members suffered injury which includes, but is not limited to,  
20 exposure to a heightened, imminent risk of fraud, identity theft, and financial harm.  
21 Plaintiffs and Class Members must monitor their financial accounts and credit  
22 histories more closely and frequently to guard against identity theft. Class  
23 Members also have incurred, and will continue to incur on an indefinite basis, out-  
24 of-pocket costs for obtaining credit reports, credit freezes, credit monitoring  
25 services, and other protective measures to deter or detect identity theft. The  
26 unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished  
27 the value of the PII.

28 98. The damages to Plaintiffs and the Class Members were a proximate,



1 reasonably foreseeable result of Equifax’s breaches of its duties.

2 99. Therefore, Plaintiffs and Class members are entitled to damages in an  
3 amount to be proven at trial.

4 **COUNT III**  
5 **NEGLIGENCE PER SE**

6 **(On behalf of the Nationwide Class and California Subclass)**

7 100. Plaintiffs incorporate by reference all paragraphs above as if fully set  
8 forth here.

9 101. Under the FCRA, 15 U.S.C. §§ 1681e, Equifax is required to “maintain  
10 reasonable procedures designed to . . . limit the furnishing of consumer reports to  
11 the purposes listed under section 1681b of this title.” 15 U.S.C. § 1681e(a).

12 102. Equifax failed to maintain reasonable procedures designed to limit the  
13 furnishing of consumer reports to the purposes outlined under section 1681b of the  
14 FCRA.

15 103. Plaintiffs and Class Members were foreseeable victims of Equifax’s  
16 violation of the FCRA. Equifax knew or should have known that a breach of its  
17 data security systems would cause damages to Class members.

18 104. As alleged above, Equifax was required under the GLBA to satisfy  
19 certain standards relating to administrative, technical, and physical safeguards:

20 **(1) to *insure the security and confidentiality of customer***  
21 ***records and information;***

22 **(2) to *protect against any anticipated threats or hazards to the***  
23 ***security or integrity of such records;* and**

24 **(3) to *protect against unauthorized access to or use of such***  
25 ***records* or information which could result in substantial harm or**  
26 **inconvenience to any customer.**

27 105. In order to satisfy their obligations under the GLBA, Equifax was also  
28 required to “develop, implement, and maintain a comprehensive information

1 security program that is [1] written in one or more readily accessible parts and [2]  
2 contains administrative, technical, and physical safeguards that are appropriate to  
3 [its] size and complexity, the nature and scope of [its] activities, and the sensitivity  
4 of any customer information at issue.” 16 C.F.R. § 314.4

5 106. In addition, under the Interagency Guidelines Establishing Information  
6 Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to  
7 “develop and implement a risk-based response program to address incidents of  
8 unauthorized access to customer information in customer information systems.”  
9 *See id.*

10 107. Further, when Equifax became aware of “unauthorized access to  
11 sensitive customer information,” it should have “conduct[ed] a reasonable  
12 investigation to promptly determine the likelihood that the information has been or  
13 will be misused” and “notif[ied] the affected customer[s] as soon as possible.” *See*  
14 *id.*

15 108. Equifax violated by GLBA by failing to “develop, implement, and  
16 maintain a comprehensive information security program” with “administrative,  
17 technical, and physical safeguards” that were “appropriate to [its] size and  
18 complexity, the nature and scope of [its] activities, and the sensitivity of any  
19 customer information at issue.” This includes, but is not limited to, Equifax’s (a)  
20 failure to implement and maintain adequate data security practices to safeguard  
21 Class Members’ PII; (b) failing to detect the Data Breach in a timely manner; and  
22 (c) failing to disclose that Equifax’s data security practices were inadequate to  
23 safeguard Class Members’ PII.

24 109. Equifax also violated the GLBA by failing to “develop and implement  
25 a risk-based response program to address incidents of unauthorized access to  
26 customer information in customer information systems.” This includes, but is not  
27 limited to, Equifax’s failure to notify appropriate regulatory agencies, law  
28 enforcement, and the affected individuals themselves of the Data Breach in a timely

1 and adequate manner.

2 110. Equifax also violated by the GLBA by failing to notify affected  
3 customers as soon as possible after it became aware of unauthorized access to  
4 sensitive customer information.

5 111. Plaintiffs and Class Members were foreseeable victims of Equifax's  
6 violation of the GLBA. Equifax knew or should have known that its failure to take  
7 reasonable measures to prevent a breach of its data security systems, and failure to  
8 timely and adequately notify the appropriate regulatory authorities, law  
9 enforcement, and Class Members themselves, would cause injury to Class  
10 Members.

11 112. Equifax's failure to comply with the applicable laws and regulations,  
12 including the FCRA and the GLBA, constitutes negligence *per se*.

13 113. But for Equifax's violation of the applicable laws and regulations,  
14 Class Members' PII would not have been accessed by unauthorized individuals.

15 114. As a result of Equifax's failure to comply with applicable laws and  
16 regulations, Plaintiffs and Class Members suffered injury which includes, but is not  
17 limited to, exposure to a heightened, imminent risk of fraud, identity theft, and  
18 financial harm. Plaintiffs and Class Members must monitor their financial accounts  
19 and credit histories more closely and frequently to guard against identity theft.  
20 Class Members also have incurred, and will continue to incur on an indefinite basis,  
21 out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring  
22 services, and other protective measures to deter or detect identity theft. The  
23 unauthorized acquisition of Plaintiffs and Class Members' PII has also diminished  
24 the value of the PII.

25 115. The damages to Plaintiffs and the Class Members were a proximate,  
26 reasonably foreseeable result of Equifax's breaches of applicable laws and  
27 regulations.

28 116. Therefore, Plaintiffs and Class members are entitled to damages in an

1 amount to be proven at trial.

2 **COUNT IV**

3 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW**

4 **Cal. Bus. & Prof. Code §§ 17200, *et seq.***

5 **(On Behalf of the Nationwide Class or, in the Alternative, the California**  
6 **Subclass)**

7 117. Plaintiffs incorporate by reference all paragraphs above as if fully set  
8 forth herein.

9 118. California Business & Professions Code § 17200 prohibits any  
10 “unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue  
11 or misleading advertising.” For the reasons discussed above, Equifax violated (and  
12 continues to violate) California’s Unfair Competition Law, California Business &  
13 Professions Code §§ 17200, *et seq.*, by engaging in the above-described unlawful,  
14 unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

15 119. Equifax’s unfair and fraudulent acts and practices include, but are not  
16 limited to, the following:

17 a. Equifax failed to enact adequate privacy and security measures,  
18 in California, to protect the Class Members’ PII from unauthorized disclosure,  
19 release, data breaches, and theft, in violation of industry standards and best  
20 practices, which was a direct and proximate cause of the Data Breach;

21 b. Equifax failed to take proper action, in California, following  
22 known security risks and prior cybersecurity incidents, which was a direct and  
23 proximate cause of the Data Breach;

24 c. Equifax knowingly and fraudulently misrepresented, in  
25 California, that they would maintain adequate data privacy and security practices  
26 and procedures to safeguard Class Members’ PII from unauthorized disclosure,  
27 release, data breaches, and theft;

28

1           d.     Equifax knowingly and fraudulently misrepresented that it did  
2 and would comply with the requirements of relevant federal and state laws  
3 pertaining to the privacy and security of Class members' PII;

4           e.     Equifax knowingly omitted, suppressed, and concealed the  
5 inadequacy of its privacy and security protections for Class Members' PII;

6           f.     Equifax failed to maintain reasonable security, in violation of  
7 Cal. Civ. Code § 1798.81.5; and

8           g.     Equifax failed to disclose the Data Breach to Class Members in a  
9 timely and accurate manner, in violation of the duties imposed by Cal. Civ. Code  
10 §§ 1798.82, *et seq.*

11         120. Equifax's acts and practices also constitute "unfair" business acts and  
12 practices, in that the harm caused by Equifax's wrongful conduct outweighs any  
13 utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral,  
14 unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused  
15 and will continue to cause substantial injury to consumers such as Plaintiffs and  
16 Class Members.

17         121. Equifax's acts and practices also constitute "unlawful" business acts  
18 and practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as  
19 described fully above), the GLBA, 15 U.S.C. § 6801 *et seq.* (as described fully  
20 above), California's fraud and deceit statutes, Cal. Civ. Code §§ 1572, 1573, 1709,  
21 1711; Cal. Bus. & Prof. Code §§ 17200, *et seq.*, 17500, *et seq.*, the California  
22 Customer Records' Act, Cal. Civ. Code §§ 1798.80, *et seq.* (as described fully  
23 below), and California common law.

24         122. There were reasonably available alternatives to further Equifax's  
25 legitimate business interests, including using best practices to protect Class  
26 Members' PII, other than Equifax's wrongful conduct described herein.

27         123. As a direct and/or proximate result of Equifax's unfair practices,  
28 Plaintiffs, the Nationwide Class, and the California Subclass have suffered injury in

1 fact in connection with the Data Breach including, but not limited to, the time and  
2 expenses related to monitoring their financial accounts for fraudulent activity, an  
3 increased, imminent risk of fraud and identity theft, and loss of value of their PII.  
4 As a result, Plaintiffs and other Class Members are entitled to compensation,  
5 restitution, disgorgement, and/or other equitable relief. Cal. Bus. & Prof. Code §  
6 17203.

7 124. Equifax knew or should have known that its data security practices and  
8 infrastructure were inadequate to safeguard Class Members' PII, and that the risk of  
9 a data breach or theft was highly likely. Equifax's actions in engaging in the above  
10 named unfair practices and deceptive acts were negligent, knowing and willful,  
11 and/or wanton and reckless with respect to Class Members' rights.

12 125. On information and belief, Equifax's unlawful and unfair business  
13 practices, except as otherwise indicated herein, continue to this day and are  
14 ongoing.

15 126. Plaintiffs and other Class Members also are entitled to injunctive relief,  
16 under California Business and Professions Code §§ 17203, 17204, to stop  
17 Equifax's wrongful acts and to require Equifax to maintain adequate security  
18 measures to protect the personal and financial information in its possession.

19 127. Under Business and Professions Code §§ 17200, *et seq.*, Plaintiffs seek  
20 restitution of money or property that Equifax may have acquired by means of  
21 Equifax's deceptive, unlawful, and unfair business practices (to be proven at trial),  
22 restitutionary disgorgement of all profits accruing to Equifax because of its  
23 unlawful and unfair business practices (to be proven at trial), declaratory relief, and  
24 attorney's fees and costs (allowed by Cal. Civ. Code Proc. §1021.5).

25 **COUNT V**

26 **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT**

27 **Cal. Civ. Code §§ 1798.80, *et seq.***

28 **(On Behalf of the California Subclass)**

1           128. Plaintiffs incorporate by reference all paragraphs above as if fully set  
2 forth herein.

3           129. “[T]o ensure that personal information about California residents is  
4 protected,” Civil Code § 1798.81.5 requires any “business that owns, licenses, or  
5 maintains personal information about a California resident [to] implement and  
6 maintain reasonable security procedures and practices appropriate to the nature of  
7 the information, to protect the personal information from unauthorized access,  
8 destruction, use, modification, or disclosure.”

9           130. Equifax owns, maintains, and licenses personal information, within the  
10 meaning of § 1798.81.5, about Plaintiffs and the California Subclass.

11           131. Equifax violated Civil Code § 1798.81.5 by failing to implement  
12 reasonable measures to protect Class Members’ PII.

13           132. As a direct and proximate result of Equifax’s violations of section  
14 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

15           133. In addition, California Civil Code § 1798.82(a) provides that “[a]  
16 person or business that conducts business in California, and that owns or licenses  
17 computerized data that includes personal information, shall disclose a breach of the  
18 security of the system following discovery or notification of the breach in the  
19 security of the data to a resident of California whose unencrypted personal  
20 information was, or is reasonably believed to have been, acquired by an  
21 unauthorized person. The disclosure shall be made in the most expedient time  
22 possible and without unreasonable delay . . . .”

23           134. Section 1798.2(b) provides that “[a] person or business that maintains  
24 computerized data that includes personal information that the person or business  
25 does not own shall notify the owner or licensee of the information of the breach of  
26 the security of the data immediately following discovery, if the personal  
27 information was, or is reasonably believed to have been, acquired by an  
28 unauthorized person.”



1 135. Equifax is a business that own or license computerized data that  
2 include personal information as defined by Cal. Civ. Code §§ 1798.80, *et seq.*

3 136. In the alternative, Equifax maintains computerized data that includes  
4 personal information that Equifax does not own as defined by Cal. Civ. Code §§  
5 1798.80, *et seq.*

6 137. Plaintiffs and the California Subclass members' PII (including, but not  
7 limited to, names, addresses, and Social Security numbers) includes personal  
8 information covered by Cal. Civ. Code § 1798.81.5(d)(1).

9 138. Because Equifax reasonably believed that Plaintiffs and the California  
10 Subclass members' personal information was acquired by unauthorized persons  
11 during the Data Breach, it had an obligation to disclose the Data Breach in a timely  
12 and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under  
13 Cal. Civ. Code § 1798.82(b).

14 139. By failing to disclose the Data Breach in a timely and accurate manner,  
15 Equifax violated Cal. Civ. Code § 1798.82.

16 140. As a direct and proximate result of Equifax's violations of sections  
17 1798.81.5 and 1798.82 of the California Civil Code, Plaintiffs and the California  
18 Subclass members suffered the damages described above including, but not limited  
19 to, time and expenses related to monitoring their financial accounts for fraudulent  
20 activity, an increased, imminent risk of fraud and identity theft, and loss of value of  
21 their PII.

22 141. Plaintiffs and the California Subclass seek relief under § 1798.84 of the  
23 California Civil Code including, but not limited to, actual damages in an amount to  
24 be proven at trial, and injunctive relief.

25 **COUNT VIVI**

26 **VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES**

27 **ACT**

28 **Cal. Civ. Code §§ 1750, *et seq.***

**(On Behalf of the California Subclass)**

1  
2 142. Plaintiffs incorporate by reference all paragraphs above as if fully set  
3 forth herein.

4 143. The Consumers Legal Remedies Act, California Civil Code §§ 1750, *et*  
5 *seq.* (the “CLRA”) has adopted a comprehensive statutory scheme prohibiting  
6 various deceptive practices in connection with the conduct of a business providing  
7 goods, property, or services to consumers primarily for personal, family, or  
8 household purposes. The self-declared purposes of the CLRA are to protect  
9 consumers against unfair and deceptive business practices and to provide efficient  
10 and economical procedures to secure such protection.

11 144. Equifax is a “person” as defined by Civil Code Section 1761(c),  
12 because Equifax is a corporation as set forth above.

13 145. Plaintiffs and Class Members are “consumers,” within the meaning of  
14 Civil Code Section 1761(d), because they are individuals who purchased products  
15 and/or services from Equifax.

16 146. Equifax performed “services,” as defined by California Civil Code  
17 Section 1761(a), with respect to its compilation, maintenance, use, and furnishing  
18 of Plaintiffs’ and California Subclass members’ PII that was compromised in the  
19 Data Breach.

20 147. Equifax’s sale of their services to other consumers and businesses in  
21 California constitutes “transaction[s]” which were “intended to result or which  
22 result[ed] in the sale” of services to consumers within the meaning of Civil Code  
23 Sections 1761(e) and 1770(a).

24 148. Plaintiffs have standing to pursue this claim as they have suffered  
25 injury in fact and have lost money as a result of Equifax’s actions as set forth  
26 herein. Specifically, Plaintiffs’ PII has been compromised and is imminently  
27 threatened with financial and identity theft, and, in fact, may have already suffered  
28 actual fraud.

1 149. Section 1770(a)(5) of the CLRA prohibits anyone from “[r]epresenting  
2 that goods or services have sponsorship, approval, characteristics, ingredients, uses,  
3 benefits, or quantities which they do not have . . . .” Equifax represented that its  
4 credit background check services would adequately secure Plaintiffs’ and  
5 California Subclass members’ PII when in fact its computer systems were  
6 inadequately protected and susceptible to breach.

7 150. Section 1770(a)(7) of the CLRA prohibits anyone from “[r]epresenting  
8 that goods or services are of a particular standard, quality, or grade, or that goods  
9 are of a particular style or model, if they are of another.” Equifax represented that  
10 its credit background check services would adequately secure Plaintiffs’ and  
11 California Subclass members’ PII when in fact its computer systems were  
12 inadequately protected and susceptible to breach.

13 151. Section 1770(a)(9) of the CLRA prohibits anyone from “[a]dvertising  
14 goods or services with intent not to sell them as advertised.” As noted above,  
15 Equifax failed to provide adequate security to the PII it was entrusted to secure for  
16 the purposes of conducting credit background checks.

17 152. A written pre-suit demand under Cal. Civ. Code § 1782(a) is  
18 unnecessary and unwarranted because Equifax has long had notice of Plaintiffs’  
19 allegations, claims and demands.

20 153. Plaintiffs, individually and on behalf of the California Subclass, seek  
21 damages, an order enjoining the acts and practices described above, and attorneys’  
22 fees and costs under the CLRA.

## 23 **VII. PRAYER FOR RELIEF**

24 Plaintiffs, on behalf of themselves and all others similarly situated, request  
25 that the Court enter judgment against Equifax as follows:

- 26 A. An order certifying this action as a class action under Federal Rule of  
27 Civil Procedure 23, defining the Class and Subclass requested herein,  
28 appointing the undersigned as Class Counsel, and finding that Plaintiffs

1 are proper representatives of the Class and Subclass requested herein;

- 2 B. Injunctive relief requiring Equifax to (1) strengthen its data security  
3 systems that maintain PII to comply with the FCRA and GLBA, the  
4 applicable state laws alleged herein (including, but not limited to, the  
5 California Customer Records Act) and best practices under industry  
6 standards; (2) engage third-party auditors and internal personnel to  
7 conduct security testing and audits on Equifax's systems on a periodic  
8 basis; (3) promptly correct any problems or issues detected by such  
9 audits and testing; and (4) routinely and continually conduct training to  
10 inform internal security personnel how to prevent, identify and contain  
11 a breach, and how to appropriately respond;
- 12 C. An order requiring Equifax to pay all costs associated with class notice  
13 and administration of class-wide relief;
- 14 D. An award to Plaintiffs and all Class (and Subclass) members of  
15 compensatory, consequential, incidental, and statutory damages,  
16 restitution, and disgorgement, in an amount to be determined at trial;
- 17 E. An award to Plaintiffs and all Class (and Subclass) members of  
18 additional credit monitoring and identity theft protection services  
19 beyond the one-year package Equifax is currently offering;
- 20 F. An award of attorneys' fees, costs, and expenses, as provided by law or  
21 equity;
- 22 G. An order requiring Equifax to pay pre-judgment and post-judgment  
23 interest, as provided by law or equity; and
- 24 H. Such other or further relief as the Court may allow.

25 **VIII. DEMAND FOR JURY TRIAL**

26 Pursuant to Federal Rule of Civil Procedure 38, Plaintiffs, individually and on  
27 behalf of the proposed classes they seek to represent, demand a jury on any issue so  
28 triable of right by a jury.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DATED: September 11, 2017

KABATECK BROWN KELLNER

By: /s/ Brian S. Kabateck

BRIAN S. KABATECK

NATALIE S. PANG

Attorneys for Plaintiffs and the Proposed  
Classes