

1 JEFFREY L. HOGUE, ESQ. (SBN#234557)  
2 TYLER J. BELONG, ESQ. (SBN#234543)  
3 ERIK A. DOS SANTOS (SBN#309998)

4 **HOGUE & BELONG**  
5 170 Laurel Street  
6 San Diego, CA 92101  
7 Telephone No: (619) 238-4720  
8 Facsimile No: (619) 270-9856

9 Attorneys for Plaintiffs

10 **UNITED STATES DISTRICT COURT**

11 **SOUTHERN DISTRICT OF CALIFORNIA**

12 OMAR SEYMORE and ANGELA )  
13 SEYMORE, individually and on )  
14 behalf of all others similarly )  
15 situated, )

16 Plaintiffs, )

17 vs. )

18 EQUIFAX, INC., a Georgia )  
19 corporation. )

20 Defendants. )  
21 )  
22 )

CASE NO.: '17CV1871 CAB MDD

**CLASS ACTION COMPLAINT FOR DAMAGES**

- 1. Violation of the Fair Credit Reporting Act (15 U.S.C. 1681, et seq.)
- 2. Negligence
- 3. Unfair and Deceptive Business Practices (Cal. Bus. & Prof. Code §§ 17200, et. seq.)
- 4. Violation of the Consumers Legal Remedies Act

**DEMAND FOR JURY TRIAL**

23  
24  
25  
26  
27  
28

1  
2 Plaintiffs, OMAR SEYMORE and ANGELA SEYMORE, individually and  
3 on behalf of all others similarly situated, and demanding trial by jury, complains and  
4 alleges upon information and belief as follows:

5 **INTRODUCTION**

6 1. This is a class action brought by Plaintiffs OMAR SEYMORE and  
7 ANGELA SEYMORE (hereinafter “PLAINTIFFS”), on behalf of themselves and  
8 others similarly situated (collectively hereinafter referred to as “PLAINTIFF  
9 CLASS”), who have sustained injuries or damages arising out of defendant,  
10 EQUIFAX, INC., a Georgia corporation’s (“EQUIFAX” or “DEFENDANT”) *inter alia*,  
11 violations of federal law and the laws of the State of California by, *inter alia*,  
12 allowing hackers to access the sensitive personal information of more than 143  
13 million people.

14 2. PLAINTIFFS petition this Court to allow them to represent and  
15 prosecute claims against DEFENDANT in class action proceedings on behalf of all  
16 those similarly situated who are residents of the State of California.

17 **JURISDICTION AND VENUE**

18 3. This class action is brought pursuant to 28 U.S.C. section 1331, as this  
19 complaint contains a federal question on its face. Moreover, this Court has diversity  
20 jurisdiction over all other claims pursuant to 28 U.S.C. section 1332(d) because  
21 PLAINTIFFS are both residents of California and Defendant is a resident of  
22 Georgia. Moreover, the amount in controversy exceeds \$5,000,000. Additionally,  
23 the Court has supplemental jurisdiction over all state law claims pursuant to 28  
24 U.S.C. section 1367 because these claims are so related to the claims arising under  
25 federal law as to form the same case or controversy under Article III of the Federal  
26 Constitution.

27 4. This Court has personal jurisdiction over DEFENDANT.  
28 DEFENDANT intentionally availed itself of the benefits of the State of California.

1 DEFENDANT does substantial business in the State of California, and it was this  
2 business that gave rise to the present claim. DEFENDANT further has sufficient  
3 minimum contacts with the State of California as to render the exercise of personal  
4 jurisdiction over this DEFENDANT proper in this state.

5 5. Venue is proper in this district pursuant to 28 U.S.C. section  
6 1391(b)(2), as a substantial part of the events or omissions giving rise to this claim  
7 occurred in San Diego. DEFENDANT has conducted substantial business in this  
8 district and a substantial portion of the property that is at issue in this action is  
9 situated in this district.

### 10 **THE PARTIES**

11 6. Plaintiff, OMAR SEYMORE is an individual and a resident of the  
12 State of California, County of San Diego.

13 7. Plaintiff, ANGELA SEYMORE is an individual and a resident of the  
14 State of California, County of San Diego.

15 8. DEFENDANT is a corporation, incorporated in Georgia, with  
16 corporate headquarters located at 1550 Peach Tree Street NW, Atlanta, Georgia,  
17 30309. DEFENDANT conducts business in the State of California.

### 18 **FACTUAL ALLEGATIONS**

19 9. DEFENDANT is one of the largest credit reporting services in the  
20 nation. They are often referred to as one of the “big three” credit reporting services.  
21 Because of their size, DEFENDANT was in possession of personal identifying  
22 information (“PII”) of hundreds of millions of Americans.

23 10. The PII that defendant possessed included individuals’ names,  
24 addresses, driver’s license numbers, credit card numbers, social security numbers,  
25 and other information contained in disputes regarding credit scores. This  
26 information can be used to, *inter alia*, open a bank account or apply for credit.  
27  
28

1 11. Plaintiffs, OMAR SEYMORE and ANGELA SEYMORE were among  
2 the individuals whose information DEFENDANT possessed.

3 12. As a consequence of the sensitive nature of the information possessed  
4 by DEFENDANT, DEFENDANT had a duty to exercise reasonable care in  
5 protecting the PII that it collected. This duty included a duty to notify individuals  
6 promptly if their PII was compromised or accessed by unauthorized third parties.  
7 DEFENDANT also had a duty to comply with all state and federal laws regarding  
8 credit reporting and the protection of consumer's personal information.

9 13. Prior to May 2017, DEFENDANT had experienced three significant  
10 security breaches in the last five years. These breaches occurred in 2013, 2016, and  
11 even as recently as January 2017.

12 14. Having suffered three previous incidents in the last five years,  
13 DEFENDANT was made acutely aware of the risk that unauthorized hackers posed  
14 to the sensitive information that DEFENDANT kept and the vulnerabilities with its  
15 cybersecurity. This pattern of successful attacks should have further put  
16 DEFENDANT on notice that its security mechanisms were inadequate. Yet,  
17 DEFENDANT failed to take subsequent action sufficient to protect this information  
18 and prevent future breaches.

19 15. On its website, DEFENDANT assured consumers that they would  
20 safeguard their information. DEFENDANT'S Privacy Policy states:

21 *We have built our reputation on our commitment to deliver reliable*  
22 *information to our customers (both businesses and consumers) and to protect*  
23 *the privacy and confidentiality of personal information about consumers. We*  
24 *also protect the sensitive information we have about businesses.*  
25 *Safeguarding the privacy and security of information, both online and offline,*  
*is a top priority for Equifax.<sup>1</sup>*

26 16. Contrary to DEFENDANT'S assurances to consumers, DEFENDANT  
27 exercised remarkably substandard cybersecurity practices. DEFENDANT'S  
28

---

<sup>1</sup> <http://www.equifax.com/privacy/>

1 cybersecurity practices were so abysmal, that United States Senator Mark R.  
2 Warner, in his September 13, 2017 letter to the Federal Trade Commission, writes:

3 Cybersecurity experts have identified a number of security lapses, including  
4 in the days following Equifax's disclosure of the breach, that potentially  
5 indicate a pattern of security failings. . . . [E]xperts have pointed to a wide  
6 range of other lapses by Equifax - including in the wake of the breach - that  
7 indicate exceptionally poor cybersecurity practices. For instance, experts have  
8 pointed to an exceedingly broad attack surface, with thousands of domains  
9 and subdomains managed by Equifax across hundreds of network hosts. And  
10 security experts have identified a range of antiquated, unpatched, or otherwise  
11 vulnerable systems maintained by Equifax.

12 Equifax's post-breach actions also raise serious concerns about the company's  
13 data security practices. For instance, Equifax chose to register a new domain,  
14 Equifaxsecurity2017.com – but not in its own name. Reports also catalogued  
15 a litany of security mistakes, including use of potentially insecure content  
16 management software and improperly configured web encryption.

17 17. Similarly, Senators Orrin G. Hatch and Ron Wyden (respectively, the  
18 Chairman and the Ranking Member of the Senate Finance Committee) submitted a  
19 joint formal inquiry to the CEO of Equifax, demanding responses to numerous very  
20 specific inquiries, and stating, “If the names, Social Security numbers, birth dates,  
21 and other information of 143 million Americans are now in the hands of  
22 cybercriminals, this breach will cause irreparable harm to programs within this  
23 Committee' s jurisdiction by way of stolen identity refund fraud, healthcare fraud,  
24 and entitlement fraud.”

25 18. As a result of DEFENDANT’s exceptionally poor cybersecurity  
26 practices, in approximately mid-May, criminal hackers gained access to the PII  
27 stored by DEFENDANT. These hackers likely collected, used, and will continue to  
28 use the personal information of around 143 million individuals. This included  
approximately 209,000 credit card numbers and dispute documents involving  
approximately 182,000 customers. These hackers had unfettered access to this  
information for at least ten weeks before the breach was discovered.

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

19. DEFENDANT claims that it was made aware of this historically massive breach on July 29, 2017. At that time, DEFENDANT did nothing to alert individuals that might have been affected of what had happened.

20. While DEFENDANT remained silent to potential victims, DEFENDANT’S executives took steps to protect themselves. Just days after the hack, on August 1, 2017 and August 2, 2017, Chief Financial Officer John Gamble, Jr., Workforce Solutions President Rodolfo Ploder, and US Information Solutions President Joseph Loughran sold a combined \$1.8 million worth of Equifax stock.

21. On September 7, 2017, DEFENDANT notified the public of the breach. This was nearly six weeks after DEFENDANT first became aware that it had occurred. In a press release, DEFENDANT stated that “Criminals exploited a U.S. website application vulnerability to gain access to certain files.”<sup>2</sup>

22. In response to this hack, DEFENDANT created a website where potentially affected consumers could enter their last name and the last six digits of their social security number in order to determine whether their information might be at risk.<sup>3</sup> But, many individuals felt uncomfortable providing even more personal information to a company that had already proven its vulnerability to secure private information.

23. On September 13, 2017, plaintiffs OMAR SEYMORE and ANGELA SEYMORE inputted their information onto this website. Each of them was informed that “*Based on the information provided, we believe that your personal information may have been impacted by this incident.*”

24. DEFENDANT also offered consumers one year of complementary identity theft protection and credit file monitoring. As stated above, however, many individuals are uncomfortable trusting DEFENDANT to protect their personal identifiers, given DEFENDANT’S gross inability to do so in the past.

---

<sup>2</sup> <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>  
<sup>3</sup> <https://www.equifaxsecurity2017.com/>

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

25. Having obtained the information stored by DEFENDANT, criminals are now able to cause a wide range of harm to PLAINTIFFS. Criminals can take out loans, create bank accounts, or mortgage property in PLAINTIFFS' names. It is also possible that those that now possess PLAINTIFFS' personal information could fraudulently obtain medical services and government benefits as well as register to vote using PLAINTIFFS' identity.

26. PLAINTIFFS will need to spend large sums of money to protect themselves due to DEFENDANT'S poor security measures. For example, PLAINTIFFS will need to closely monitor their financial accounts and utilize professional services in order to detect whether their identity is stolen. They will also need to need to freeze lines of credit that they have already taken out. If their identity is eventually stolen, they will expend the time and bear the responsibility of correcting it, to the extent doing so is even possible.

27. This burden will continue indefinitely for PLAINTIFFS. With such a treasure trove of information available, wrongdoers can afford to be patient. For the rest of their lives, PLAINTIFFS will always carry with them the fear that somebody else has their personal information, and will attempt to use it against their interest.

28. DEFENDANT either knew or should have known of the potentially disastrous results that would follow a security breach of this scale. As a leader in the credit reporting sector, DEFENDANT is well aware of the many possible illegitimate uses that a person with bad intentions would have for the information of another. As a result, DEFENDANT should have done more to protect the personal information that it was charged with storing.

///  
///  
///  
///



**CLASS ALLEGATIONS**

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

29. PLAINTIFFS bring this action pursuant to Federal Rule of Civil Procedure 23, seeking both injunctive and monetary relief. PLAINTIFFS bring this suit individually, and on behalf of all others similarly situated, with PLAINTIFFS proceeding as the representative members of the proposed classes below:

The “**Nationwide Class**” consists of all individuals and entities residing in the United States of America whose personal identifiable information was compromised by Equifax’s data breach announced on September 7, 2017.

The “**California Class**” consists of all individuals and entities residing in the State of California whose personal identifiable information was compromised by Equifax’s data breach announced on September 7, 2017.

30. Notwithstanding the class definitions provided in Paragraph 27, the following individuals shall not be a member of either class: all attorneys for the class, Equifax and any entities over which Equifax has a controlling interest, and any judge to whom this action is assigned including their staff and immediate family members.

**RULE 23(a)**

31. **Numerosity.** The persons who comprise the PLAINTIFF CLASS are so numerous that the joinder of all such persons would be unfeasible and impracticable. The membership of the entire class is unknown to PLAINTIFF at this time; however, the PLAINTIFF, based on information and belief, alleges that the number of potential members in the PLAINTIFF CLASS is sufficient to satisfy numerosity, and the identity of such membership is readily ascertainable via inspection of DEFENDANT’S business records. It is believed that there are more than 143 million members of the nationwide class, and tens of millions of members



1 of the California class.

2 32. **Commonality.** This class action presents several questions of law and  
3 fact that will be common to all members of the class. These include:

- 4 a. Whether DEFENDANTS' business practices as alleged herein is a  
5 violation under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, et  
6 seq.;
- 7 b. Whether DEFENDANT acted negligently in storing and protecting  
8 the Personal Identifying Information of PLAINTIFFS and the  
9 PLAINTIFF CLASS;
- 10 c. Whether DEFENDANT'S alleged negligence with regard to  
11 PLAINTIFFS' and the PLAINTIFF CLASS' information caused  
12 PLAINTIFF and members of the PLAINTIFF CLASS to suffer  
13 damages;
- 14 d. Whether PLAINTIFF and the PLAINTIFF CLASS is entitled to  
15 injunctive relief;
- 16 e. Whether the DEFENDANTS' business practices as alleged herein  
17 constitute an unfair, unlawful, or fraudulent business practice in  
18 violation of California Business & Professions Code §17200, et.  
19 seq.;
- 20 Whether DEFENDANTS' business practices as alleged herein is a  
21 violation under the Consumers Legal Remedies Act, Cal. Civil Code  
22 §§ 17500, et seq.;

23  
24 33. **Typicality.** The claims or defenses of the PLAINTIFFS are typical of  
25 the claims or defenses of the class. PLAINTIFFS' information was stolen by  
26 hackers as a result of DEFENDANT'S inadequate methods for securing  
27 information. The PLAINTIFF CLASS claims that their information was also stolen  
28 as a result of the same deficiencies.

1           34. The relief sought by PLAINTIFFS is the same relief sought by the  
2 PLAINTIFF CLASS.

3           35. **Adequacy.** The PLAINTIFFS will fairly and adequately protect the  
4 interests of the class. PLAINTIFFS seek the same relief for both themselves and the  
5 class. Their interests are perfectly aligned. Both the PLAINTIFF and the  
6 PLAINTIFF CLASS seek to hold DEFENDANT responsible for its extensive  
7 wrongdoing under the same theories. It is in PLAINTIFFS' best interest to  
8 prosecute these claims fully and to obtain all compensation to which they are  
9 rightfully entitled.

10           36. PLAINTIFFS have retained experienced class counsel to prosecute this  
11 lawsuit. Class counsel have both the knowledge and experience to handle a matter  
12 of this complexity.

13           37. **Superiority.** Under the facts and circumstances set forth above, class  
14 action proceedings are superior to any other methods available for both fair and  
15 efficient adjudication of the rights of each PLAINTIFF CLASS member inasmuch  
16 as joinder of individual members of the PLAINTIFF CLASS is not practical. Even  
17 if joinder were practical, said PLAINTIFF CLASS members could not individually  
18 afford the litigation relative to their individual potential recoveries, meaning that  
19 individual litigation would be inappropriately burdensome, not only to said citizens,  
20 but also the courts of the nation.

21           38. To process individual cases would increase both the expenses and the  
22 delay not only to PLAINTIFF CLASS members, but also to DEFENDANTS and the  
23 Court. In contrast, a class action of this matter will avoid case management  
24 difficulties and provide multiple benefits to the litigating parties, including  
25 efficiency, economies of scale, unitary adjudication with consistent results and equal  
26 protection of the rights of each PLAINTIFF CLASS member, all by way of the  
27 comprehensive and efficient supervision of the litigation by a single court.  
28

1 **RULE 23(b)**

2 39. DEFENDANT has acted, or refused to act, on grounds that are  
3 generally applicable to the entire class, such that final injunctive relief or  
4 corresponding declaratory relief is appropriate respecting the class as a whole.

5 40. The above referenced questions of law or fact common to all class  
6 members will predominate over individual members, such that a class action is  
7 superior to other available methods for fairly and efficiently adjudicating the  
8 controversy. DEFENDANT’S lack of data security put all of the data that it held at  
9 risk. When hackers were able to defeat the measures that were place, they were able  
10 to gain access to all class members’ data at the same time. Thus, common issues  
11 relating to DEFENDANT’S failure to safeguard all class members’ information will  
12 overwhelm any individual questions.

13  
14 **RULE 23(c)**

15 41. Pursuant to Fed. Rule Civ. Proc. 23(c)(4), the Court may certify only  
16 particular issues for class treatment.

17  
18 **COUNTS**

19  
20 **COUNT 1: VIOLATION OF THE FAIR CREDIT REPORTING ACT (15**  
21 **U.S.C. § 1681 ET. SEQ.)**

22 42. PLAINTIFFS and the PLAINTIFF CLASS incorporate all the  
23 preceding paragraphs as if fully set forth herein.

24 43. Congress enacted the Fair Credit Reporting Act in order to ensure the  
25 accuracy and fairness of credit reporting. 15 U.S.C. § 1561(a). This legislation  
26 sought to create a statutory scheme that was “fair and equitable to the consumer,  
27 with regard to the confidentiality, accuracy, relevancy, and proper utilization” of  
28 information used to make decisions regarding the extension of credit. 15 U.S.C. §

1 1681(b) (emphasis added.)

2 44. The Fair Credit Reporting Act defines a consumer as an individual. (15  
3 U.S.C. § 1681a(c). The PLAINTIFFS and all members of the PLAINTIFF CLASS  
4 are thus consumers, entitled to protection.

5 45. A consumer reporting agency is defined to mean “any person which,  
6 for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in  
7 whole or in part in the practice of assembling or evaluating consumer credit  
8 information or other information on consumers for the purpose of furnishing  
9 consumer reports to third parties, and which uses any means or facility of interstate  
10 commerce for the purpose of preparing or furnishing consumer reports.” 15 U.S.C. §  
11 1681a(f). A person is defined broadly to include “any individual, partnership,  
12 corporation, trust, estate, cooperative, association, government or governmental  
13 subdivision or agency, or other entity.” 15 U.S.C. § 1681a(b).

14 46. DEFENDANT is a consumer reporting agency under the definition  
15 provided by this statute because DEFENDANT is multi-billion-dollar company that  
16 almost exclusively assembles and evaluates consumer credit information or other  
17 information on consumers for the purpose of furnishing reports to third parties.

18 47. 15 U.S.C. § 1681(b) lists the permissible purposes for consumer reports  
19 and specifies that these are the only uses to which these reports may lawfully put.  
20 This section *does not* include giving information to hackers with potentially criminal  
21 intentions. A consumer credit report is defined to mean “written, oral, or other  
22 communication of any information by a consumer reporting agency bearing on a  
23 consumer's credit worthiness [creditworthiness], credit standing, credit capacity,  
24 character, general reputation, personal characteristics, or mode of living which is  
25 used or expected to be used or collected in whole or in part for the purpose of  
26 serving as a factor in establishing the consumer's eligibility for... (A) credit or  
27 insurance to be used primarily for personal, family, or household purposes... (B)  
28 employment purposes; or... (C) any other purpose authorized under section 604.” 15

1 U.S.C. § 1681a(d).

2 48. The information that hackers were able to access was a consumer report  
3 under this statute because it was a communication of information relating to a  
4 consumer's creditworthiness, credit standing, credit capacity, character, general  
5 reputation, personal characteristics, or mode of living and was expected to be used  
6 in deciding whether to extend credit to a consumer. The only reason that  
7 DEFENDANT had for collecting this information in the first place was to use it to  
8 create reports for this purpose, as doing so was DEFENDANT'S primary business.

9 49. As a consumer reporting agency, DEFENDANT was obligated by 15  
10 U.S.C §1681(e) to maintain reasonable procedures designed to limit use of those  
11 reports to the uses described in section 1681b.

12 50. DEFENDANT did not comply with the requirements of the Fair Credit  
13 Reporting Act because DEFENDANT unreasonably allowed unauthorized  
14 individuals to gain access to consumer reports that it was tasked with protecting.  
15 Despite suffering multiple breaches in the past, DEFENDANT did not take the  
16 action that was necessary to protect these reports from coming into the hands of  
17 those that would misuse them.

18 51. DEFENDANT willfully and/or recklessly violated the provisions of §§  
19 1681b and 1681e by allowing other parties to access the personal information of  
20 more than 143 million consumers. The nature of DEFENDANT'S conduct is shown  
21 by the lack of response to previous hacks, its Privacy Policy explicitly recognizing  
22 the importance of data security, the actions of DEFENDANT'S executives in selling  
23 their stock immediately after this breach occurred, and DEFENDANT'S intentional  
24 and prolonged delay in announcing this breach to the public.

25 52. Further, any reasonable credit reporting agency would have been aware  
26 of the importance of safeguarding confidential information. These agencies  
27 distribute information to other entities, so that these entities can use the information  
28 to make important decisions. As a result, they were aware of the power that an

1 individual could wield if they were to obtain the personal information of another and  
2 attempt to use it for nefarious purposes.

3 53. PLAINTIFFS and the PLAINTIFF CLASS have suffered damages as a  
4 result of DEFENDANT’S willful and/or reckless failure to comply the Fair Credit  
5 Reporting Act. Therefore, PLAINTIFFS and the PLAINTIFF CLASS are entitled  
6 to damages of not less than \$100 and not more than \$1,000. 15 U.S.C. §  
7 1681n(a)(1). Additionally, PLAINTIFFS and PLAINTIFF CLASS are entitled to  
8 punitive damages, costs, and reasonable attorneys’ fees. 15 U.S.C. § 1681n(a)(2)  
9 and (3).

10 54. In the alternative, DEFENDANTS acted negligently in violating the  
11 Fair Credit Reporting Act, because their lack of reasonable care caused  
12 PLAINTIFFS and the PLAINTIFF CLASS’S personal information to be used for  
13 purposes other than those described in section 1681b. PLAINTIFFS and  
14 PLAINTIFF CLASS are entitled to their actual damages, costs, and reasonable  
15 attorney’s fees. 15 U.S.C. § 1681o.

16  
17 **COUNT TWO: NEGLIGENCE**

18 55. PLAINTIFFS and the PLAINTIFF CLASS incorporate all the  
19 preceding paragraphs as if fully set forth herein.

20 56. DEFENDANT owed a duty to PLAINTIFF and the PLAINTIFF  
21 CLASS to exercise reasonable care in protecting their personal information.  
22 DEFENDANT’S duty included, among other things, designing, maintaining,  
23 monitoring, and testing all security systems in order to guarantee that all sensitive  
24 information was sufficiently protected.

25 57. DEFENDANT’S Privacy Policy explicitly acknowledged the nature of  
26 this duty.

27 58. DEFENDANT had a duty to take steps to promptly and effectively  
28 detect any intrusion of its data systems that might occur.

1           59.    DEFENDANT had a duty to delete PII that was no longer needed to  
2 serve client needs.

3           60.    DEFENDANT had a duty to inform consumers that its data security  
4 practices were inadequate to protect PLAINTIFFS and the PLAINTIFF CLASS'  
5 PII.

6           61.    PLAINTIFFS and the PLAINTIFF CLASS reposed a special trust in  
7 DEFENDANT by virtue of the fact that DEFENDANT was in possession of  
8 PLAINTIFFS' and the PLAINTIFF CLASS' PII. This trust gave rise to an  
9 independent duty of care. DEFENDANT was a multi-billion-dollar company with  
10 experience handling sensitive information, and thus should have had the ability to  
11 protect the data that it stored from attack.

12           62.    DEFENDANT breached its duty of care in multiple ways. Defendant  
13 failed to implement and maintain adequate procedures in order to safeguard  
14 PLAINTIFFS' and the PLAINTIFF CLASS' PII. DEFENDANT further failed to  
15 inform PLAINTIFFS and the PLAINTIFF CLASS that it did not have the ability to  
16 guarantee the safety of their PII. Once the breach occurred, DEFENDANT failed to  
17 promptly detect the breach. Finally, once DEFENDANT did detect the breach, it  
18 failed to notify PLAINTIFFS or the PLAINTIFF CLASS of what had happened in a  
19 timely manner.

20           63.    But for DEFENDANT'S breach of duty, PLAINTIFF and the  
21 PLAINTIFF CLASS' PII would not have been compromised or obtained by  
22 hackers.

23           64.    Given the prior security breaches that had occurred, it was reasonably  
24 foreseeable that another security breach could occur and that people's credit could  
25 be affected if DEFENDANT did not increase its cybersecurity. Further,  
26 PLAINTIFFS and the PLAINTIFF CLASS members were foreseeable plaintiffs  
27 because DEFENDANT were in possession of their PII.  
28



1           65. As a result of DEFENDANT’S failure to protect the PII that it stored,  
2 PLAINTIFFS and the PLAINTIFF CLASS have suffered injury. These individuals’  
3 information will remain at risk for the rest of their lives. Apart from the emotional  
4 stress of knowing that they are vulnerable to identity theft at any time, they will  
5 need to carefully monitor both their credit score and all other financial accounts in  
6 order to prevent misuse of their information. They will forever be subject to a  
7 heightened risk of fraud, and will need to take steps in order to protect themselves.  
8 Further, if their identity is subsequently stolen, they will need to act in order to  
9 minimize and reverse the damage to the extent possible. Accomplishing these tasks  
10 will require professional assistance that PLAINTIFFS and the PLAINTIFF CLASS  
11 will need to pay for out of pocket. These costs will continue to be incurred into the  
12 indefinite future.

13           66. The damages to PLAINTIFFS and the PLAINTIFF CLASS were a  
14 proximate and readily foreseeable result of DEFENDANT’S breach of duty.

15           67. Therefore, PLAINTIFFS and the PLAINTIFF CLASS are entitled to  
16 damages in an amount to be proven at trial.

17           **COUNT THREE: UNFAIR AND DECEPTIVE BUSINESS PRACTICES**  
18           **(CAL. BUS. & PROF. CODE §§ 17200 ET. SEQ.)**

19           68. PLAINTIFFS and the PLAINTIFF CLASS incorporate all the  
20 preceding paragraphs as if fully set forth herein.

21           69. Beginning at an exact date unknown to PLAINTIFFS and the  
22 PLAINTIFF CLASS, but within the past four years, the DEFENDANTS have  
23 committed acts of unfair, unlawful, and fraudulent conduct, as defined by California  
24 Business & Professions Code section 17200, as set forth in this Complaint.

25           70. Plaintiff alleges that DEFENDANTS’ actions were unlawful,  
26 deceptive, and misleading.

27           71. DEFENDANT has violated California law, including the California  
28 Customer Records Act (Cal. Civ. Code § 1798.80 et. seq.). That statute requires that

1 “A business that owns, licenses, or maintains personal information about a  
2 California resident shall implement and maintain reasonable security procedures and  
3 practices appropriate to the nature of the information, to protect the personal  
4 information from unauthorized access, destruction, use, modification, or disclosure.”  
5 Cal. Civ. Code § 1798.81.5.

6 72. DEFENDANT violated the California Customer Records Act by failing  
7 to implement reasonable security procedures and practices appropriate to this sort of  
8 incredibly sensitive and incredibly confidential information. Defendant’s  
9 shortcomings caused personal information of approximately 143 million people to  
10 fall into the hands of hackers. DEFENDANT had suffered previous security  
11 breaches in the past, and knew that its system was weak, but did not take the steps  
12 necessary to fix it.

13 73. In addition to the failure to prevent the breach of its security systems,  
14 DEFENDANT also failed to timely notify those that would be impacted of what had  
15 happened. Once DEFENDANT did notify PLAINTIFFS and the PLAINTIFF  
16 CLASS that their information had been compromised, the only remedy that  
17 DEFENDANT offered required PLAINTIFF and the PLAINTIFF CLASS to  
18 provide DEFENDANT with even more personal information.

19 74. As a proximate result of the above-mentioned acts of defendants,  
20 PLAINTIFF and the PLAINTIFF CLASS have lost money or property and suffered  
21 injury in fact, and have been damaged in a sum according to proof at the time of  
22 trial.

23 75. If not stopped, DEFENDANT will continue to inure benefit from their  
24 unlawful, unfair, and fraudulent acts.

25 76. PLAINTIFF is informed, believes, and thereon alleges that these acts of  
26 the DEFENDANT were willful, oppressive, fraudulent, and malicious in that  
27 DEFENDANT knew that its security systems had been breached multiple times in  
28 the past, but did not act to shore them up. DEFENDANT also failed to inform

1 consumers of the breach so that they could protect themselves. Instead,  
2 DEFENDANT’S executives sold their own stock so that they would not be harmed  
3 when it plummeted in value.

4 77. DEFENDANT had a profit-based motive to act in the manner alleged.  
5 Updating security systems in order to be able to protect the vast amounts of data  
6 stored by DEFENDANT would have likely been costly. Once the breach had  
7 occurred, DEFENDANT could not reveal what had happened out of fear that its  
8 reputation would be negatively impacted. Because it is essential that the public trust  
9 DEFENDANT with their information, the fallout from this incident could have been  
10 devastating.

11 78. Accordingly, the PLAINTIFFS and the PLAINTIFF CLASS are  
12 entitled to punitive and exemplary damages, to deter such future conduct, in an  
13 amount within the jurisdiction of the Superior Court to be proved at the time of trial.

14 **COUNT FOUR: VIOLATION OF THE CONSUMER LEGAL REMEDIES**  
15 **ACT (CALIFORNIA CIVIL CODE §§ 1750, ET. SEQ.)**

16 79. PLAINTIFFS and the PLAINTIFF CLASS incorporate all the  
17 preceding paragraphs as if fully set forth herein.

18 80. DEFENDANT’S actions toward PLAINTIFF and the PLAINTIFF  
19 CLASS, as set forth above, constitute unfair and deceptive acts or practices in  
20 violation of applicable law, including the Consumers Legal Remedies Act,  
21 California Civil Code section 1770(a)(5), (7), and (9), which provide, in pertinent  
22 part, that “the following unfair methods of competition and unfair or deceptive acts  
23 or practices undertaken by any person in a transaction intended to result or which  
24 results in the sale or lease of goods or services to any consumer are unlawful:...

- 25 a. Representing that goods or services have sponsorship, approval,  
26 characteristics, ingredients, uses, benefits, or quantities that they do  
27 not have or that a person has a sponsorship, approval, status,  
28

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

affiliation, or connection that he or she does not have.

- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another.
- c. Advertising goods or services with intent not to sell them as advertised.”

81. PLAINTIFF is informed and believes and thereon alleges that the above described unfair and deceptive practices were intentionally adopted by DEFENDANT in order to enhance DEFENDANT income by allowing them to avoid costs associated with maintaining a security system that would adequately protect the personal information that DEFENDANT possessed, and avoid losing revenue as a result of a diminished reputation once the public learned what had happened.

**PRAYER FOR RELIEF**

WHEREFORE, the PLAINTIFFS and the PLAINTIFF CLASS:

- 1. For an Order that the action be certified as a class action;
- 2. For an Order that Plaintiffs be appointed representatives of the Class;
- 3. For and Order that the attorneys of record for Plaintiffs be appointed Class Counsel;
- 4. Pursuant to California Business & Professions Code §§17203 & 17535, and pursuant to the court’s equitable powers, Plaintiffs pray that the DEFENDANT be ordered to restore to the general public all funds acquired by means of any act or practice declared by the Court to be unlawful, unfair or fraudulent or to constitute unfair advertising under §17500;

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

5. For an order awarding PLAINTIFF and the PLAINTIFF CLASS pre-judgment and post-judgment interest as well as their reasonable attorney’s fees and costs pursuant the Consumer Legal Remedies Act, Civil Code §§ 1750, et seq.; Code of Civil Procedure §1021.5; and other statutes as may be applicable;
6. For costs of suit; and
7. For all such other and further relief the Court may deem just and proper.

Dated: September 13, 2017

**HOGUE & BELONG**

By: s/ Jeffrey L. Hogue  
JEFFREY L. HOGUE  
TYLER J. BELONG  
ERIK A. DOS SANTOS  
Attorneys for Plaintiffs

CIVIL COVER SHEET

17CV1871 CAB MDD

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS
Omar Seymore, Angela Seymore
(b) County of Residence of First Listed Plaintiff San Diego
(c) Attorneys (Firm Name, Address, and Telephone Number)
Jeffrey L. Hogue, Tyler J. Belong
170 Laurel Street
San Diego, CA 92101; (619) 238-4720

DEFENDANTS
EQUIFAX, INC., a Georgia corporation
County of Residence of First Listed Defendant Fulton, Georgia
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.
Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)
1 U.S. Government Plaintiff
2 U.S. Government Defendant
3 Federal Question (U.S. Government Not a Party)
4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
PTF DEF
Citizen of This State
Citizen of Another State
Citizen or Subject of a Foreign Country
Incorporated or Principal Place of Business In This State
Incorporated and Principal Place of Business In Another State
Foreign Nation

IV. NATURE OF SUIT (Place an "X" in One Box Only)
CONTRACT
PERSONAL INJURY
REAL PROPERTY
CIVIL RIGHTS
PRISONER PETITIONS
FORFEITURE/PENALTY
LABOR
IMMIGRATION
BANKRUPTCY
PROPERTY RIGHTS
SOCIAL SECURITY
FEDERAL TAX SUITS
OTHER STATUTES

V. ORIGIN (Place an "X" in One Box Only)
1 Original Proceeding
2 Removed from State Court
3 Remanded from Appellate Court
4 Reinstated or Reopened
5 Transferred from Another District (specify)
6 Multidistrict Litigation - Transfer
8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
15 U.S.C. 1681, et seq
Brief description of cause:
Violation of the Fair Credit Reporting Act resulting from data breach by defendant.

VII. REQUESTED IN COMPLAINT:
CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.
DEMAND \$
CHECK YES only if demanded in complaint:
JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY
(See instructions):
JUDGE
DOCKET NUMBER

DATE
09/13/2017
SIGNATURE OF ATTORNEY OF RECORD
/s Jeffrey L. Hogue

FOR OFFICE USE ONLY
RECEIPT #
AMOUNT
APPLYING IFP
JUDGE
MAG. JUDGE