

1 GIRARDI AND KEESE  
 2 THOMAS V. GIRARDI, State Bar No. 36603  
 3 ROBERT W. FINNERTY, State Bar No. 119775  
 4 CHRISTOPHER T. AUMAIS, State Bar No. 249901  
 5 1126 Wilshire Boulevard  
 6 Los Angeles, California 90017  
 7 Telephone: (213) 977-0211  
 8 Facsimile: (213) 481-1554

9 [Additional Counsel appear on signature  
 10 page]

11 Attorneys for Plaintiffs and the Putative  
 12 Class

13 UNITED STATES DISTRICT COURT  
 14 CENTRAL DISTRICT OF CALIFORNIA – WESTERN DIVISION

15 AMANDA JANAYE WHITE, and  
 16 ROBERT HONANIAN, individually  
 17 and on behalf of all others similarly  
 18 situated,

19 Plaintiffs,

20 v.

21 EQUIFAX, INC., a Georgia  
 22 corporation,

23 Defendant.

CASE NO. 2:17-cv-07991

**CLASS ACTION COMPLAINT**

1. WILLFUL VIOLATION OF FAIR CREDIT REPORTING ACT
2. NEGLIGENT VIOLATION OF FAIR CREDIT REPORTING ACT
3. NEGLIGENCE
4. NEGLIGENCE PER SE
5. VIOLATION OF STATE DATA BREACH STATUTES
6. VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE § 17200 - UNLAWFUL BUSINESS PRACTICES
7. VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §17200 UNFAIR BUSINESS PRACTICES
8. VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §17200 FRAUDULENT/DECEPTIVE BUSINESS PRACTICES

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

9. DECLARATORY JUDGMENT  
**JURY TRIAL DEMANDED**

Plaintiffs Amanda Janaye White, and Robert Honanian, (hereinafter, “Plaintiff” or “Plaintiffs”), individually and on behalf of the Classes defined below, alleges the following against Equifax, Inc. (“Equifax”) based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of publicly available documents as to all other matters:

**INTRODUCTION**

1. Plaintiffs brings this class action case against Equifax for its gross and systemic failures to secure and safeguard consumers’ personally identifiable information (“PII”) which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate and adequate notice to Plaintiffs and other Class members that their PII had been stolen and precisely what types of information were stolen.

2. Equifax has acknowledged that a cybersecurity incident (“Data Breach”) potentially impacting approximately 143 million U.S. consumers occurred. It has also acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. By

1 Equifax's own admission, the information accessed primarily includes names, Social  
2 Security numbers, birth dates, addresses and some driver's license numbers. Equifax  
3  
4 has also confirmed that credit card numbers for approximately 209,000 U.S. consumers,  
5 and certain dispute documents with personal identifying information for approximately  
6 182,000 U.S. consumers, were stolen.  
7

8 3. Equifax learned of the Data Breach on July 29 2017, but failed to disclose  
9 it to affected consumers and the public at large until September 7, 2017. Instead, three  
10 senior Equifax executives sold at least \$1.8 million worth of shares before the public  
11 disclosure of the breach.  
12

13 4. The PII for Plaintiffs and the class of consumers they seek to represent was  
14 compromised due to Equifax's acts and omissions and their failure to properly protect  
15 the PII.  
16

17 5. Equifax could have prevented this Data Breach. Data breaches at other  
18 companies, including one of its major competitors, Experian have occurred.  
19

20 6. The Data Breach was the inevitable result of Equifax's inadequate  
21 approach to data security and the protection of the PII that it collected during the course  
22 of its business.  
23

24 7. Equifax disregarded the rights of Plaintiffs and Class members by  
25 intentionally, willfully, recklessly, or negligently failing to take adequate and  
26 reasonable measures to ensure its data systems were protected, failing to disclose to its  
27 customers the material fact that it did not have adequate computer systems and security  
28

1 practices to safeguard PII, failing to take available steps to prevent and stop the breach  
2 from ever happening, and failing to monitor and detect the breach on a timely basis.

3  
4 8. As a result of the Equifax Data Breach, the PII of the Plaintiffs and Class  
5 members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs  
6 and Class members, or likely to be suffered by Plaintiffs and Class members as a direct  
7 and proximate result of the Equifax Data Breach include: (a) theft of their personal and  
8 financial information; (b) costs associated with the detection and prevention of identity  
9 theft and unauthorized use of their financial accounts; (c) costs associated with time  
10 spent and the loss of productivity from taking time to address and attempt to ameliorate,  
11 mitigate, and deal with the actual and future consequences of the data breach, including  
12 finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring  
13 and identity theft protection services, imposition of withdrawal and purchase limits on  
14 compromised accounts, and the stress, nuisance, and annoyance of dealing with all  
15 issues resulting from the Data Breach; (d) the imminent and certainly impending injury  
16 flowing from potential fraud and identify theft posed by their personal and financial  
17 information being placed in the hands of hackers; (e) damages to, and diminution in  
18 value of, their personal and financial information entrusted to Equifax for the sole  
19 purpose of Equifax's credit-reporting services and with the mutual understanding that  
20 Equifax would safeguard Plaintiff's and Class members' data against theft and not  
21 allow access and misuse of their data by others; (f) money paid to Equifax for credit-  
22 reporting services during the period of the Data Breach in that Plaintiff and Class  
23  
24  
25  
26  
27  
28

1 members would not have obtained, or permitted others to obtain, Equifax's credit-  
2 reporting services had Equifax disclosed that it lacked adequate systems and procedures  
3 to reasonably safeguard consumers' financial and personal information and had Equifax  
4 provided timely and accurate notice of the Data Breach; (g) overpayments paid to  
5 Equifax for credit-reporting services in that a portion of the price paid by Plaintiffs and  
6 the Class, or others on their behalf, to Equifax was for the costs of Equifax providing  
7 reasonable and adequate safeguards and security measures to protect customers'  
8 financial and personal data, which Equifax did not do, and as a result, Plaintiffs and  
9 members of the Class did not receive what was paid for and Equifax overcharged for  
10 these services; and (h) continued risk to their financial and personal information, which  
11 remains in the possession of Equifax and which is subject to further breaches so long as  
12 Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs' and  
13 Class members' PII in its possession.

14  
15  
16  
17  
18 9. The injuries to the Plaintiffs and Class members were directly and  
19 proximately caused by Equifax's failure to implement or maintain adequate data  
20 security measures for PII.

21  
22 10. Further, Plaintiffs retains a significant interest in ensuring that their PII,  
23 which, while stolen, remains in the possession of Equifax is protected from further  
24 breaches, and seeks to remedy the harms they have suffered on behalf of themselves  
25 and similarly situated consumers whose PII was stolen as a result of the Equifax Data  
26 Breach.  
27  
28



1 Equifax regularly transacts business in this District, and hundreds of thousands of the  
2 Class members, including Plaintiff, reside in this District. The cause of actions for  
3 hundreds of thousands of putative class members also arose, in part, in this District.  
4

5 **PARTIES**

6 15. Plaintiff Amanda Janaye White resides in Riverside County, California,  
7 and is a California citizen. Following the disclosure of the Data Breach, White  
8 accessed Equifax's website, [www.trustedidpremier.com](http://www.trustedidpremier.com), inputting her last name and six  
9 digits from her social security number as instructed, and received a response indicating  
10 that Equifax believes her personal information was impacted by the Data Breach.  
11  
12

13 16. Plaintiff Robert Honanian resides in Los Angeles County, California, and  
14 is a California citizen. Following the disclosure of the Data Breach, Honanian accessed  
15 Equifax's website, [www.trustedidpremier.com](http://www.trustedidpremier.com), inputting his last name and six digits  
16 from his social security number as instructed, and received a response indicating that  
17 Equifax believes his personal information was impacted by the Data Breach.  
18  
19

20 17. Plaintiffs' personal and financial information was compromised as a result  
21 of Equifax's failures and gross misconduct that resulted in the Data Breach. Plaintiffs  
22 were harmed and sustained actual, concrete damages by having their financial and  
23 personal information compromised by the Data Breach.  
24

25 18. Plaintiffs would not have provided, or would not have authorized others to  
26 provide, their personal and financial information to Equifax in connection with credit-  
27 reporting services had Equifax disclosed that it lacked adequate computer systems and  
28

1 data security practices to safeguard consumers’ personal and financial information from  
2 hacking and theft.

3  
4 19. Plaintiffs suffered actual and concrete injury as a result of Equifax’s  
5 systemic failures and gross misconduct that resulted in the Data Breach.

6  
7 20. Defendant Equifax, Inc. is a Delaware corporation with its principal place  
8 of business located in Atlanta, Georgia. It provides credit information services to  
9 millions of business, governmental units, and consumers throughout the world.  
10 Equifax operates through various subsidiaries and agents, each of which entities acted  
11 as agents of Equifax, or in the alternative, in concert with Equifax.  
12

13 **CLASS ACTION ALLEGATIONS**

14 21. Plaintiffs seek relief on behalf of themselves and as representatives of all  
15 others who are similarly situated.  
16

17 **A. Nationwide Class**

18 22. Plaintiffs asserts statutory claims under the Fair Credit Reporting Act and  
19 common law claims for negligence on behalf of all U.S. consumers defined as follows:  
20

21 All persons residing in the United States whose personally identifiable  
22 information (PII) was accessed, compromised, or acquired by  
23 unauthorized persons in the Equifax Data Breach first disclosed on or  
24 about September 7, 2017 (the “Nationwide Class”).

25 **B. Statewide Classes**

26 23. Plaintiffs assert statutory claims under the laws of various individual  
27 states, and on behalf of separate statewide classes, defined as follows:  
28

1 All persons residing in [STATE] whose PII was accessed, compromised,  
2 or acquired by unauthorized persons in the Equifax Data Breach first  
3 disclosed on or about September 7, 2017 (the “Statewide Classes”).

4 **C. California Subclass**

5 24. Plaintiff also assert statutory claims under California’s Unfair Competition  
6 Law on behalf of all California consumers defined as follows:

7  
8 All persons residing in California whose PII was accessed,  
9 compromised, or acquired by unauthorized persons in the Equifax Data  
10 Breach first disclosed on or about September 7, 2017 (the “California  
Subclass”).

11 25. Excluded from the Nationwide Class, the Statewide Classes, and the  
12 California Subclass (collectively, the “Classes”) are Equifax, its affiliates, parents or  
13 subsidiaries, its officers, directors and members of their immediate families and any  
14 entity in which Equifax has a controlling interest, the legal representatives, heirs,  
15 successors or assigns of any such excluded party, all persons who make a timely  
16 election to be excluded from the Class, government entities; and the judicial officer(s)  
17 to whom this case is assigned, and the members of their immediate families.  
18

19  
20 26. Plaintiffs reserve the right to amend or modify the definition of the  
21 proposed Classes if necessary after having had an opportunity to conduct discovery.  
22

23 27. Each of the proposed Classes meets the criteria for certification under  
24 Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3).  
25

26 28. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the Class are so  
27 numerous that the joinder of each member is impractical. By Equifax’s own admission,  
28

1 the Classes consist of approximately 143 million members, the identity of whom are  
2 well within the knowledge of and can be ascertained by resort to Equifax's records. In  
3 fact, Equifax's [www.trustedidpremier.com](http://www.trustedidpremier.com) website already maintains the identities of  
4 these class members, demonstrating Equifax has the administrative capability through  
5 its computer systems and other records to identify all members of the Classes, and such  
6 specific information is not otherwise available to Plaintiff.  
7  
8

9       29. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed.  
10 R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves  
11 common questions of law and fact that predominate over any questions affecting  
12 individual Class members. The common questions include:  
13

- 14       a. Whether Equifax engaged in the wrongful conduct alleged herein;
- 15       b. Whether Equifax owed a duty to Plaintiffs and members of the  
16 Classes to adequately protect their PII;
- 17       c. Whether Equifax owed a duty to Plaintiffs and members of the  
18 Classes to provide timely and accurate notice of the Data Breach to  
19 Plaintiffs and members of the Classes;
- 20       d. Whether Equifax breached its duty to Plaintiffs and members of the  
21 Classes by failing to provide adequate data security;
- 22       e. Whether Equifax breached its duty to Plaintiffs and members of the  
23 Classes by failing to provide timely and accurate notice of the Data  
24 Breach to Plaintiffs and members of the Classes;
- 25       f. Whether Equifax knew or should have known that their data  
26 security systems were highly vulnerable to attack;
- 27       g. Whether Equifax unlawfully failed to disclose that it did not  
28 maintain computers and security practices adequate to reasonably  
safeguard consumers' financial and personal data;

- 1 h. Whether Equifax's security measures to protect their systems were  
2 reasonable in light of the measures recommended by data security  
3 experts;
- 4 i. Whether Equifax was negligent in failing to implement reasonable  
5 and adequate security procedures and practices;
- 6 j. Whether Equifax's failure to implement adequate data security  
7 measures allowed the breach to occur;
- 8 k. Whether Equifax's conduct was deceptive, unfair, unconscionable,  
9 and/or unlawful;
- 10 l. Whether Equifax's conduct, including their failure to act, resulted  
11 in or was the proximate cause of the breach of its systems, resulting  
12 in the loss of the PII of Plaintiffs and members of the Classes;
- 13 m. Whether Plaintiffs and members of the Classes suffered injured,  
14 including ascertainable losses, as a result of Equifax's conduct (or  
15 failure to act);
- 16 n. Whether Plaintiffs and members of the Classes are entitled to  
17 recover monetary relief; and
- 18 o. Whether Plaintiffs and members of the Classes are entitled to  
19 equitable relief, including declaratory and injunctive relief,  
20 restitution, disgorgement, and/or other equitable relief.

21 30. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P.  
22 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had  
23 their PII compromised in the Data Breach. Plaintiffs' damages and injuries are akin to  
24 other Class members and Plaintiffs seek relief consistent with the relief of the Class.

25 31. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiffs are an adequate  
26 representative of the Class because Plaintiffs are members of the Class and are  
27 committed to pursuing this matter against Equifax to obtain relief for the Class.  
28 Plaintiffs have no conflicts of interest with the Class and have retained competent

1 counsel experienced in the prosecution of class actions. Plaintiffs intend to vigorously  
2 prosecute this case and will fairly and adequately protect the Class' interests.

3  
4 32. **Superiority. Fed. R. Civ. P. 23(b)(3).** A class action is superior to any  
5 other available means for the fair and efficient adjudication of this controversy, and no  
6 unusual difficulties are likely to be encountered in the management of this class action.  
7  
8 The quintessential purpose of the class action mechanism is to permit litigation against  
9 wrongdoers even when damages to individual Plaintiffs may not be sufficient to justify  
10 individual litigation. Here, the damages suffered by Plaintiffs and the Class are  
11 relatively small compared to the burden and expense required to individually litigate  
12 their claims against Equifax, and thus, individual litigation to redress Equifax's  
13 wrongful conduct would be impracticable. Individual litigation by each Class member  
14 would also strain the court system. Individual litigation creates the potential for  
15 inconsistent or contradictory judgments, and increases the delay and expense to all  
16 parties and the court system. By contrast, the class action device presents far fewer  
17 management difficulties and provides the benefits of a single adjudication, economies  
18 of scale, and comprehensive supervision by a single court.  
19  
20  
21

22 33. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2) and (c).** The  
23 requirements of Fed. R. Civ. P. 23(b)(2) and (c) are also met because Equifax, through  
24 its uniform conduct, has acted or refused to act on grounds generally applicable to the  
25 Classes, making injunctive and declaratory relief appropriate for the Classes as a whole.  
26  
27  
28

1 **STATEMENT OF FACTS**

2 34. Equifax is one of three nationwide credit-reporting companies that tracks  
3 and rates the financial history of U.S. consumers. The companies are supplied with  
4 data about loans, loan payments and credit cards, as well as information on everything  
5 from child support payments, credit limits, missed rent and utilities payments,  
6 addresses and employer history. All of this information, and more, factors into  
7 consumers' credit scores.  
8

9  
10 35. Unlike other data breaches, not all of the people affected by the Equifax  
11 breach may be aware that they are customers of the company. Equifax gets its data  
12 from credit card companies, banks, retailers, and lenders who report on the credit  
13 activity of individuals to credit reporting agencies, as well as by purchasing public  
14 records.  
15

16  
17 36. According to Equifax's report on September 7, 2017, the breach was  
18 discovered on July 29th. The perpetrators gained access by "[exploiting] a [...] website  
19 application vulnerability" on one of the company's U.S.-based servers. The hackers  
20 were then able to "gain access to certain files." See  
21 <https://www.equifaxsecurity2017.com/> (last visited September 22, 2017).  
22  
23

24 37. Included among those files was a treasure trove of personal data: names,  
25 dates of birth, Social Security numbers and addresses. In some cases -- Equifax states  
26 around 209,000 -- the records also included actual credit card numbers. Documentation  
27 about disputed charges was also leaked. Those documents contained additional  
28

1 personal information on around 182,000 Americans.

2 38. Personal data like this is a major score for cybercriminals who will likely  
3  
4 look to capitalize on it by launching targeted phishing campaigns.

5 39. Plaintiffs suffered actual injury in the form of damages to and diminution  
6 in the value of their PII – a form of intangible property that Plaintiffs entrusted to  
7  
8 Equifax and that was compromised in and as a result of the Equifax Data Breach.

9 40. Additionally, Plaintiffs have suffered imminent and impending injury  
10 arising from the substantially increased risk of future fraud, identity theft and misuse  
11  
12 posed by their PII being placed in the hands of criminals who have already, or will  
13 imminently, misuse such information.

14 41. Moreover, Plaintiffs have a continuing interest in ensuring that his private  
15 information, which remains in the possession of Equifax, is protected and safeguarded  
16  
17 from future breaches.

18 42. At all relevant times, Equifax knew, or reasonably should have known,  
19  
20 that the PII it collected, maintained and stored is highly sensitive, susceptible to attack,  
21 and could be used for wrongful purposes by third parties, such as identity theft and  
22  
23 fraud.

24 43. Equifax recognized its obligation to maintain the security of U.S.  
25 consumers' PII and financial information in its Privacy Policy:

26  
27 For more than 100 years, Equifax has been a catalyst for commerce by  
28 bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.

1  
2 We have built our reputation on our commitment to deliver reliable  
3 information to our customers (both businesses and consumers) and to  
4 protect the privacy and confidentiality of personal information about  
5 consumers. We also protect the sensitive information we have about  
6 businesses. Safeguarding the privacy and security of information, both  
7 online and offline, is a top priority for Equifax

8 See <http://www.equifax.com/privacy/> (last visited September 22, 2017).

9 44. Equifax further promises to consumers that “[w]e will not disclose your  
10 personal information to third parties except to provide you with the disclosure or  
11 service you request . . .” See <http://www.equifax.com/privacy/personal-credit-reports>  
12 (last visited September 22, 2017). Equifax also promises that it is “committed to  
13 protecting the security of your information through procedures and technology  
14 designed for this purpose.” *Id.*

15 45. It is well known and the subject of many media reports that PII is highly  
16 coveted and a frequent target of hackers. Despite the frequent public announcements of  
17 data breaches of corporate entities, including Experian, Equifax maintained an  
18 insufficient and inadequate system to protect the PII of Plaintiffs and Class members.  
19

20 46. Although Equifax claims to be a leader in data security and its privacy  
21 policy promises to reasonably safeguard consumer data, Equifax’s own data security  
22 practices were inadequate. Equifax was well aware of this fact because it had  
23 experienced multiple data breaches in recent years.  
24

25 47. 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  
28

1 consumer credit reports using sufficient personal information to bypass Equifax's  
2 identity verification process. *See* Letter from Troy G. Kubes, Vice President &  
3 Associate Group Counsel at Equifax Legal Department, to Attorney General Joseph  
4 Foster, March 5, 2014, [https://www.doj.nh.gov/consumer-security-](https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf)  
5 [breaches/documents/equifax-20140305.pdf](https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf) (last visited September 22, 2017).  
6

7  
8 48. In May 2016, Equifax's W-2 Express website suffered a data breach where  
9 an attacker was able to access, download and post the names, addresses, social security  
10 numbers and other personal information of over 430,000 Kroger employees. The  
11 attackers were able to access the W-2 data by merely entering Equifax's portal with an  
12 employee's default PIN code, which was the last four digits of the employee's Social  
13 Security number and their four-digit birth year. *See* Crooks Grab W-2s from Credit  
14 Bureau Equifax, Krebs on Security, [http://krebsonsecurity.com/2016/05/crooks-grab-w-](http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/)  
15 [2s-from-credit-bureau-equifax/](http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/) (last visited September 22, 2017).  
16  
17

18 49. Independent security researchers have also found that Equifax's website is  
19 vulnerable. In 2016, a security researcher found a common vulnerability known as  
20 cross-site scripting (XSS) on the main Equifax website. Such XSS bugs allow attackers  
21 to send specially-crafted links to Equifax customers and, if the target clicks through and  
22 is logged into the site, their username and password can be revealed to the hacker. *See*  
23  
24 A Brief History of Equifax Security Fails, Forbes,  
25 [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)  
26 [history/#53a60715677c](https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#53a60715677c) (last visited September 22, 2017).  
27  
28

1           50.     Researcher Kenneth White just recently discovered a link in the source  
2 code on the Equifax consumer sign-in page that pointed to Netscape, a web browser  
3 that was discontinued in 2008. Kevin Beaumont, a British security professional, found  
4 decade-old software in use, including IBM WebSphere, Apache Struts and Java, many  
5 of which are outdated and subject to well-known vulnerabilities. *Id.*  
6

7  
8           51.     Given its critical role in credit markets, and the vast amounts of the most  
9 detailed PII and financial information of U.S. consumers that can be easily used by  
10 hackers or customers of hackers to prey on innocent consumers by using their identities  
11 and credit, Equifax was aware of the need to have the most current protective measures  
12 in place to prevent a hack and to minimize the impact of a hack should an intrusion  
13 occur. It is incomprehensible that Equifax had such poor protections and systems in  
14 place to allow hackers to infiltrate the PII and financial information of 143 million U.S.  
15 consumers for well over a month before being detected.  
16  
17

18           52.     On September 13, 2017, Equifax confirmed that there was a vulnerability  
19 in its systems called Apache Struts CV-2017-5638. *See*  
20 <https://www.equifaxsecurity2017.com/> (last visited on September 22, 2017).  
21 According to the Apache Software Foundation, the software company that Equifax used  
22 to build the website that was hacked, the Data Breach occurred due to Equifax's failure  
23 to install security updates to a server that it received from Apache in a timely manner.  
24 See <https://blogs.apache.org/foundation/date/20170914> (last visited on September 25,  
25 2017). That vulnerability was well known to Equifax in early March 2017, when a  
26  
27  
28

1 security patch was issued. Yet, shockingly, Equifax failed to install the patch, leaving  
2 its web server unsecure.

3  
4 53. PII is a valuable commodity because it contains not only payment card  
5 numbers but PII as well. A “cyber blackmarket” exists in which criminals openly post  
6 stolen payment card numbers, social security numbers, and other personal information  
7 on a number of underground Internet websites. PII is “as good as gold” to identity  
8 thieves because they can use victims’ personal data to open new financial accounts and  
9 take out loans in another person’s name, incur charges on existing accounts, or clone  
10 ATM, debit, or credit cards.  
11

12  
13 54. Social Security numbers are a particularly popular target for hackers.  
14 Combinations of Social Security numbers, birth dates and names sell for more than  
15 credit card numbers in an increasingly sophisticated black market, where such  
16 information is sold and resold through popular auction sites.  
17

18  
19 55. Legitimate organizations and the criminal underground alike recognize the  
20 value in PII contained in a merchant’s data systems; otherwise, they would not  
21 aggressively seek or pay for it. For example, in “one of 2013’s largest breaches . . . not  
22 only did hackers compromise the [card holder data] of three million customers, they  
23 also took registration data [containing PII] from 38 million users.” *See* Verizon 2014  
24 PCI Compliance Report, available at:  
25 [http://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/retail/verizon\\_pci2014.pdf](http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf)  
26  
27 (hereafter “2014 Verizon Report”), at 54 (last visited September 20, 2017).  
28

1           56. At all relevant times, Equifax knew, or reasonably should have known, of  
2 the importance of safeguarding PII and of the foreseeable consequences that would  
3 occur if its data security system was breached, including, specifically, the significant  
4 costs that would be imposed on individuals as a result of a breach.  
5

6           57. Equifax was, or should have been, fully aware of the significant number of  
7 people whose PII it collected, and thus, the significant number of individuals who  
8 would be harmed by a breach of Equifax's systems.  
9

10           58. Unfortunately, and as alleged below, despite all of this publicly available  
11 knowledge of the continued compromises of PII in the hands of other third parties,  
12 Equifax's approach to maintaining the privacy and security of the PII of Plaintiffs and  
13 Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.  
14  
15

16           59. The ramifications of Equifax's failure to keep Plaintiffs' and Class  
17 members' data secure are severe.  
18

19           60. The FTC defines identity theft as "a fraud committed or attempted using  
20 the identifying information of another person without authority." 17 C.F.R § 248.201  
21 (2013). The FTC describes "identifying information" as "any name or number that may  
22 be used, alone or in conjunction with any other information, to identify a specific  
23 person." *Id.*  
24

25           61. Personal identifying information (PII) is a valuable commodity to identity  
26 thieves once the information has been compromised. As the FTC recognizes, once  
27 identity thieves have personal information, "they can drain your bank account, run up  
28

1 your credit cards, open new utility accounts, or get medical treatment on your health  
2 insurance.” Federal Trade Commission, Warning Signs of Identity Theft, available at:  
3 <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited  
4 September 20, 2017).  
5

6 62. Identity thieves can use personal information, such as that of Plaintiffs and  
7 Class members which Equifax failed to keep secure, to perpetrate a variety of crimes  
8 that harm victims. For instance, identity thieves may commit various types of  
9 government fraud such as: immigration fraud; obtaining a driver’s license or  
10 identification card in the victim’s name but with another’s picture; using the victim’s  
11 information to obtain government benefits; or filing a fraudulent tax return using the  
12 victim’s information to obtain a fraudulent refund.  
13  
14  
15

16 63. Javelin Strategy and Research reports that identity thieves have stolen  
17 \$112 billion in the past six years. See [https://www.javelinstrategy.com/coverage-](https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point)  
18 [area/2016-identity-fraud-fraud-hits-inflection-point](https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point) (last visited September 20, 2017).  
19

20 64. Reimbursing a consumer for a financial loss due to fraud does not make  
21 that individual whole again. On the contrary, identity theft victims must spend  
22 numerous hours and their own money repairing the impact to their credit. After  
23 conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”)  
24 found that identity theft victims “reported spending an average of about 7 hours  
25 clearing up the issues” and resolving the consequences of fraud in 2014. Victims of  
26 Identity Theft, 2014 (Sept. 2015) available at:  
27  
28

1 <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited September 20, 2017).

2           65. There may be a time lag between when harm occurs versus when it is  
3 discovered, and also between when PII or PCD is stolen and when it is used. According  
4 to the U.S. Government Accountability Office (“GAO”), which conducted a study  
5 regarding data breaches:  
6

7           [L]aw enforcement officials told us that in some cases, stolen data may be  
8 held for up to a year or more before being used to commit identity theft.  
9 Further, once stolen data have been sold or posted on the Web, fraudulent  
10 use of that information may continue for years. As a result, studies that  
11 attempt to measure the harm resulting from data breaches cannot  
necessarily rule out all future harm.

12 GAO, Report to Congressional Requesters, at 29 (June 2007), available at

13 <http://www.gao.gov/new.items/d07737.pdf> (last visited September 20, 2017)

14           66. Plaintiffs and Class members now face years of constant surveillance of  
15 their financial and personal records, monitoring, and loss of rights. The Class is  
16 incurring and will continue to incur such damages in addition to any fraudulent use of  
17 their PII.  
18

19           67. The PII of Plaintiffs and Class members is private and sensitive in nature  
20 and was left inadequately protected by Equifax. Equifax did not obtain Plaintiffs’ and  
21 Class members’ consent to disclose their PII to any other person as required by  
22 applicable law and industry standards.  
23

24           68. The Equifax Data Breach was a direct and proximate result of Equifax’s  
25 failure to properly safeguard and protect Plaintiffs’ and Class members’ PII from  
26  
27  
28

1 unauthorized access, use, and disclosure, as required by various state and federal  
2 regulations, industry practices, and the common law, including Equifax's failure to  
3 establish and implement appropriate administrative, technical, and physical safeguards  
4 to ensure the security and confidentiality of Plaintiffs' and Class members' PII to  
5 protect against reasonably foreseeable threats to the security or integrity of such  
6 information.  
7  
8

9       69. Equifax had the resources to prevent a breach, but neglected to adequately  
10 invest in data security, despite the growing number of well-publicized data breaches.  
11

12       70. Had Equifax remedied the deficiencies in its data security systems,  
13 followed security guidelines, and adopted security measures recommended by experts  
14 in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of  
15 its customers' PII.  
16

17       71. As a direct and proximate result of Equifax's wrongful actions and  
18 inaction and the resulting Data Breach, Plaintiffs and Class members have been placed  
19 at an imminent, immediate, and continuing increased risk of harm from identity theft  
20 and identity fraud, requiring them to take the time which they otherwise would have  
21 dedicated to other life demands such as work and effort to mitigate the actual and  
22 potential impact of the Data Breach on their lives including, inter alia, by placing  
23 "freezes" and "alerts" with credit reporting agencies, contacting their financial  
24 institutions, closing or modifying financial accounts, closely reviewing and monitoring  
25 their credit reports and accounts for unauthorized activity, and filing police reports.  
26  
27  
28

1 This time has been lost forever and cannot be recaptured. In all manners of life in this  
2 country, time has constantly been recognized as compensable, for many consumers it is  
3 the way they are compensated, and even if retired from the work force, consumers  
4 should be free of having to deal with the consequences of a credit reporting agency's  
5 slippage, as is the case here.  
6

7  
8 72. Equifax's wrongful actions and inaction directly and proximately caused  
9 the theft and dissemination into the public domain of Plaintiffs' and Class members'  
10 PII, causing them to suffer, and continue to suffer, economic damages and other actual  
11 harm for which they are entitled to compensation, including:  
12

- 13 a. Theft of their personal and financial information;
- 14 b. Unauthorized charges on their debit and credit card accounts;
- 15 c. The imminent and certainly impending injury flowing from  
16 potential fraud and identity theft posed by their PII being placed in  
17 the hands of criminals and already misused via the sale of  
18 Plaintiffs' and Class members' information on the black market;
- 19 d. The untimely and inadequate notification of the Data Breach;
- 20 e. The improper disclosure of their PII;
- 21 f. Loss of privacy;
- 22 g. Ascertainable losses in the form of out-of-pocket expenses and the  
23 value of their time reasonably incurred to remedy or mitigate the  
24 effects of the Data Breach;
- 25 h. Ascertainable losses in the form of deprivation of the value of their  
26 PII and PCD, for which there is a well-established national and  
27 international market;
- 28 i. Ascertainable losses in the form of the loss of cash back or other  
benefits as a result of their inability to use certain accounts and

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

cards affected by the Data Breach;

- j. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,
- k. The loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

73. Equifax has not offered customers any meaningful credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiffs and Class members, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiffs or Class members.

74. Experts are now recommending that all Americans whose PII is impacted by the Data Breach should freeze their credit with all three of the major credit reporting agencies, Equifax, Experian, and TransUnion. There are financial costs associated with

1 freezing and unfreezing a consumer's credit report, further compounding the actual and  
2 concrete damages that Plaintiffs and the Classes have and will sustain. Even if a less  
3 onerous lock is placed on the credit report, members of the Classes have been advised  
4 to regularly monitor activity on their credit reports to determine whether any nefarious  
5 conduct has occurred which would require a locking of their credit. *See*  
6 <https://www.transunion.com/credit-freeze/place-credit-freeze2> (last visited September  
7  
8 22, 2017).

9  
10 75. While the PII of Plaintiffs and members of the Class has been stolen,  
11 Equifax continues to hold PII of consumers, including Plaintiffs and Class members.  
12 Particularly because Equifax and has demonstrated an inability to prevent a breach or  
13 stop it from continuing even after being detected, Plaintiffs and members of the Class  
14 have an undeniable interest in insuring that their PII is secure, remains secure, is  
15 properly and promptly destroyed and is not subject to further theft.  
16  
17

18  
19 **COUNT I**  
20 **WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT**  
21 **(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR,**  
22 **ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE**  
23 **CLASSES)**

24 76. Plaintiffs restate and reallege Paragraphs 1 through 74 as if fully set forth  
25 here.

26 77. This is a claim for relief under the Fair Credit Reporting Act ("FRCA"), 11  
27 U.S.C. § 1681, *et seq.*

28 78. As individuals, Plaintiffs and Class members are consumers entitled to the

1 protections of the FCRA. 15 U.S.C. § 1681a(c).

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

7  
8  
9           80. Equifax is a consumer reporting agency under the FCRA because, for  
10 monetary fees, it regularly engages in the practice of assembling or evaluating  
11 consumer credit information or other information on consumers to furnish consumer  
12 reports to third parties evaluating the consumers’ credit for varying purposes.

13  
14           81. As a consumer reporting agency, the FCRA requires Equifax to “maintain  
15 reasonable procedures designed to . . . limit the furnishing of consumer reports to the  
16 purposes listed under section 1681b of this title.” 15 U.S.C. § 1681e(a).

17  
18           82. Under the FCRA, a “consumer report” is defined as “any written, oral, or  
19 other communication of any information by a consumer reporting agency bearing on a  
20 consumer’s credit worthiness, credit standing, credit capacity, character, general  
21 reputation, personal characteristics, or mode of living which is used or expected to be  
22 used or collected in whole or in part for the purpose of serving as a factor in  
23 establishing the consumer’s eligibility for -- (A) credit . . . to be used primarily for  
24 personal, family, or household purposes; . . . or (C) any other purpose authorized under  
25 section 1681b of this title.” 15 U.S.C. § 1681a(d)(1).  
26  
27  
28

1           83. The compromised data was a consumer report under the FCRA because it  
2 was a communication of information bearing on Class members' credit worthiness,  
3 credit standing, credit capacity, character, general reputation, personal characteristics,  
4 or mode of living used, or expected to be used or collected in whole or in part, for the  
5 purpose of serving as a factor in establishing the Class members' eligibility for credit.  
6

7  
8           84. As a consumer reporting agency, Equifax may only furnish a consumer  
9 report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other."  
10 15 U.S.C. § 1681b(a).  
11

12           85. None of the purposes listed under 15 U.S.C. § 1681b permit credit  
13 reporting agencies to furnish consumer reports to unauthorized or unknown entities, or  
14 computer hackers such as those who accessed the Nationwide Class members' PII.  
15 Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown  
16 entities or computer hackers, as detailed above.  
17

18           86. Equifax furnished the Nationwide Class members' consumer reports by  
19 disclosing their consumer reports to unauthorized entities and computer hackers;  
20 allowing unauthorized entities and computer hackers to access their consumer reports;  
21 knowingly and/or recklessly failing to take security measures that would prevent  
22 unauthorized entities or computer hackers from accessing their consumer reports;  
23 and/or failing to take reasonable security measures that would prevent unauthorized  
24 entities or computer hackers from accessing their consumer reports.  
25  
26  
27

28           87. The Federal Trade Commission ("FTC") has pursued enforcement actions

1 against consumer reporting agencies under the FCRA for failing to “take adequate  
2 measures to fulfill their obligations to protect information contained in consumer  
3 reports, as required by the” FCRA, in connection with data breaches.

4  
5 88. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by  
6 providing impermissible access to consumer reports and by failing to maintain  
7 reasonable procedures designed to limit the furnishing of consumer reports to the  
8 purposes outlined under section 1681b of the FCRA. The willful and reckless nature of  
9 Equifax’s violations is supported by, among other things, former employees’  
10 admissions that Equifax’s data security practices have deteriorated in recent years, and  
11 Equifax’s numerous other data breaches in the past. Further, Equifax touts itself as an  
12 industry leader in breach prevention; thus, Equifax was well aware of the importance of  
13 the measures organizations should take to prevent data breaches, and willingly failed to  
14 take them.  
15  
16  
17

18 89. Equifax also acted willfully and recklessly because it knew or should have  
19 known about its legal obligations regarding data security and data breaches under the  
20 FCRA. These obligations are well established in the plain language of the FCRA and  
21 in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804  
22 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part  
23 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available these and  
24 other substantial written materials that apprised them of their duties under the FCRA.  
25 Any reasonable consumer reporting agency knows or should know about these  
26  
27  
28

1 requirements. Despite knowing of these legal obligations, Equifax acted consciously in  
2 breaching known duties regarding data security and data breaches and depriving  
3 Plaintiffs and members of the Nationwide Class of their rights under the FCRA.  
4

5 90. Equifax’s willful and/or reckless conduct provided a means for  
6 unauthorized intruders to obtain and misuse Plaintiffs’ and members of Nationwide  
7 Class members’ personal information for no permissible purposes under the FCRA.  
8

9 91. Plaintiffs and members of the Nationwide Class have been damaged by  
10 Equifax’s willful or reckless failure to comply with the FCRA.  
11

12 92. Plaintiffs and members of the Nationwide Class are therefore entitled to  
13 recover “any actual damages sustained by the consumer . . . or damages of not less than  
14 \$100 and not more than \$1,000.” 15 U.S.C. § 1681n(a)(1)(A).  
15

16 93. Plaintiffs and members of the Nationwide Class are also entitled to  
17 punitive damages, costs of the action, and reasonable attorneys’ fees. 15 U.S.C.  
18 §1681n(a)(2) & (3).  
19

20 **COUNT II**  
21 **NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**  
22 **(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR,**  
23 **ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE**  
24 **CLASSES)**

25 94. Plaintiffs restate and reallege Paragraphs 1 through 74 and 76 through 86  
26 as if fully set forth herein.

27 95. This is a claim for relief under the Fair Credit Reporting Act (“FRCA”), 11  
28 U.S.C. § 1681, *et seq.*



1 safeguard that information and to use commercially reasonable methods to do so.  
2 Equifax knew that the PII was private and confidential and should be protected as  
3 private and confidential.  
4

5 104. Equifax owed a duty of care not to subject Plaintiffs, along with their PII,  
6 and Class members to an unreasonable risk of harm because they were foreseeable and  
7 probable victims of any inadequate security practices.  
8

9 105. Equifax owed numerous duties to Plaintiffs and to members of the  
10 Nationwide Class, including the following:  
11

- 12 a. To exercise reasonable care in obtaining, retaining, securing,  
13 safeguarding, deleting and protecting PII in its possession;
- 14 b. To protect PII using reasonable and adequate security procedures  
15 and systems that are compliant with industry-standard practices;  
16 and
- 17 c. To implement processes to quickly detect a data breach and to  
18 timely act on warnings about data breaches.

19 106. Equifax also breached its duty to Plaintiffs and the Class members to  
20 adequately protect and safeguard PII by knowingly disregarding standard information  
21 security principles, despite obvious risks, and by allowing unmonitored and unrestricted  
22 access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide  
23 adequate supervision and oversight of the PII with which they were and are entrusted,  
24 in spite of the known risk and foreseeable likelihood of breach and misuse, which  
25 permitted an unknown third party to gather PII of Plaintiffs and Class members, misuse  
26 the PII and intentionally disclose it to others without consent.  
27  
28

1           107. Equifax knew, or should have known, of the risks inherent in collecting  
2 and storing PII, the vulnerabilities of its data security systems, and the importance of  
3 adequate security. Equifax knew about numerous, well-publicized data breaches,  
4 including the breach at Experian.

6           108. Equifax knew, or should have known, that their data systems and networks  
7 did not adequately safeguard Plaintiffs' and Class members' PII.

9           109. Equifax breached its duties to Plaintiffs and Class members by failing to  
10 provide fair, reasonable, or adequate computer systems and data security practices to  
11 safeguard PII of Plaintiffs and Class members.

13           110. Because Equifax knew that a breach of its systems would damage millions  
14 of individuals, including Plaintiffs and Class members, Equifax had a duty to  
15 adequately protect their data systems and the PII contained thereon.

17           111. Equifax had a special relationship with Plaintiffs and Class members.  
18 Plaintiffs' and Class members' willingness to entrust Equifax with their PII was  
19 predicated on the understanding that Equifax would take adequate security precautions.  
20 Moreover, only Equifax had the ability to protect its systems and the PII it stored on  
21 them from attack.

23           112. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs  
24 and Class members and their PII. Equifax's misconduct included failing to: (1) secure  
25 its systems, despite knowing their vulnerabilities, (2) comply with industry standard  
26 security practices, (3) implement adequate system and event monitoring, and (4)  
27 security practices, (3) implement adequate system and event monitoring, and (4)  
28 security practices, (3) implement adequate system and event monitoring, and (4)

1 implement the systems, policies, and procedures necessary to prevent this type of data  
2 breach.

3  
4 113. Equifax also had independent duties under state and federal laws that  
5 required Equifax to reasonably safeguard Plaintiffs' and Class members' Personal  
6 Information and promptly notify them about the data breach.

7  
8 114. Equifax breached its duties to Plaintiffs and Class members in numerous  
9 ways, including:

- 10 a. By failing to provide fair, reasonable, or adequate computer  
11 systems and data security practices to safeguard PII of Plaintiffs  
12 and Class members;
- 13 b. By creating a foreseeable risk of harm through the misconduct  
14 previously described;
- 15 c. By failing to implement adequate security systems, protocols and  
16 practices sufficient to protect Plaintiffs' and Class members' PII  
17 both before and after learning of the Data Breach;
- 18 d. By failing to comply with the minimum industry data security  
19 standards during the period of the Data Breach; and
- 20 e. By failing to timely and accurately disclose that Plaintiffs' and  
21 Class members' PII had been improperly acquired or accessed.

22 115. Through Equifax's acts and omissions described in this Complaint,  
23 including Equifax's failure to provide adequate security and its failure to protect PII of  
24 Plaintiffs and Class members from being foreseeably captured, accessed, disseminated,  
25 stolen and misused, Equifax unlawfully breached its duty to use reasonable care to  
26 adequately protect and secure PII of Plaintiffs and Class members during the time it  
27 was within Equifax's possession or control.  
28

1           116. The law further imposes an affirmative duty on Equifax to timely disclose  
2 the unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs  
3 and Class members can take appropriate measures to mitigate damages, protect against  
4 adverse consequences, and thwart future misuse of their PII.  
5

6           117. Equifax breached its duty to notify Plaintiffs and Class members of the  
7 unauthorized access by waiting many months after learning of the breach to notify  
8 Plaintiff and Class members and then by failing to provide Plaintiffs and Class  
9 members information regarding the breach until September 2017. Instead, its  
10 executives disposed of at least \$1.8 million worth of shares in the company after  
11 Equifax learned of the data breach but before it was publicly announced. To date,  
12 Equifax has not provided sufficient information to Plaintiffs and Class members  
13 regarding the extent of the unauthorized access and continues to breach its disclosure  
14 obligations to Plaintiffs and the Class.  
15  
16  
17

18           118. Through Equifax's acts and omissions described in this Complaint,  
19 including Equifax's failure to provide adequate security and its failure to protect PII of  
20 Plaintiffs and Class members from being foreseeably captured, accessed, disseminated,  
21 stolen and misused, Equifax unlawfully breached its duty to use reasonable care to  
22 adequately protect and secure PII of Plaintiffs and Class members during the time it  
23 was within Equifax's possession or control.  
24  
25

26           119. Further, through its failure to provide timely and clear notification of the  
27 Data Breach to consumers, Equifax prevented Plaintiffs and Class members from  
28

1 taking meaningful, proactive steps to secure their financial data and bank accounts.

2           120. Upon information and belief, Equifax improperly and inadequately  
3 safeguarded PII of Plaintiffs and Class members in deviation of standard industry rules,  
4 regulations, and practices at the time of the unauthorized access. Equifax's failure to  
5 take proper security measures to protect sensitive PII of Plaintiffs and Class members  
6 as described in this Complaint, created conditions conducive to a foreseeable,  
7 intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class  
8 members.  
9  
10

11           121. Equifax's conduct was grossly negligent and departed from all reasonable  
12 standards of care, including, but not limited to: failing to adequately protect the PII;  
13 failing to conduct regular security audits; failing to provide adequate and appropriate  
14 supervision of persons having access to PII of Plaintiffs and Class members; and failing  
15 to provide Plaintiffs and Class members with timely and sufficient notice that their  
16 sensitive PII had been compromised.  
17  
18

19           122. Neither Plaintiffs nor the other Class members contributed to the Data  
20 Breach and subsequent misuse of their PII as described in this Complaint.  
21

22           123. Equifax's Data Breach proximately caused Plaintiffs and Nationwide Class  
23 members to be exposed to fraud and to be harmed. The injuries suffered by the  
24 Plaintiffs and members of the Nationwide Class are a direct result of Equifax's breach  
25 of its duties and include: theft of their PII and financial information; costs associated  
26 with the detection and prevention of identity theft and unauthorized use of their  
27  
28

1 financial accounts; costs associated with time spent and the loss of productivity from  
2 taking time to address and attempt to ameliorate, mitigate, and deal with the actual and  
3 potential consequences of the Data Breach, including closely reviewing and monitoring  
4 their credit reports and accounts for unauthorized activity, finding fraudulent charges,  
5 cancelling and reissuing cards, closing or modifying financial accounts, purchasing  
6 credit monitoring and identity theft protection services, placing “freezes” and “alerts”  
7 with credit reporting agencies, contacting their financial institutions, imposition of  
8 withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and  
9 annoyance of dealing with all issues resulting from the Data Breach, which may take  
10 months if not years to discover and detect, given the far-reaching, adverse and  
11 detrimental consequences of identity theft and loss of privacy; the imminent and  
12 certainly impending injury flowing from potential fraud and identify theft posed by  
13 their PII and financial information being placed in the hands of hackers; damages to  
14 and diminution in value of their PII and financial information entrusted to Equifax for  
15 the sole purpose of Equifax’s credit-reporting services and with the mutual  
16 understanding that Equifax would safeguard Plaintiffs’ and Nationwide Class members’  
17 data against theft and not allow access and misuse of their data by others; money paid  
18 to Equifax for their services during the period of the Data Breach in that Plaintiffs and  
19 members of the Nationwide Class would not have obtained, or permitted others to  
20 obtain, Equifax’s credit-reporting services had Equifax disclosed that it lacked adequate  
21 systems and procedures to reasonably safeguard consumers’ PII and financial  
22  
23  
24  
25  
26  
27  
28

1 information and had Equifax provided timely and accurate notice of the Data Breach;  
2 payments made to Equifax for credit reporting services in that a portion of the price  
3 paid by Plaintiffs and the Nationwide Class, or others on their behalf, to Equifax was  
4 for the costs of Equifax providing reasonable and adequate safeguards and security  
5 measures to protect customers' PII and financial data and, as a result, Plaintiffs and  
6 members of the Nationwide Class did not receive what was bargained and paid for; and  
7 continued risk to Plaintiffs and members of the Nationwide Class that their PII and  
8 financial information, which remains in the possession of Equifax and which is subject  
9 to further breaches so long as Equifax fails to undertake appropriate and adequate  
10 measures to protect it; damages arising from the unauthorized charges on their debit or  
11 credit cards or on cards that were fraudulently obtained through the use of the PII of  
12 Plaintiffs and Class members; damages from lost time and effort to mitigate the actual  
13 and potential impact of the Data Breach on their lives including, inter alia, by placing  
14 "freezes" and "alerts" with credit reporting agencies, contacting their financial  
15 institutions, closing or modifying financial accounts, closely reviewing and monitoring  
16 their credit reports and accounts for unauthorized activity, and filing police reports and  
17 damages from identity theft, which may take months if not years to discover and detect,  
18 given the far-reaching, adverse and detrimental consequences of identity theft and loss  
19 of privacy. The nature of other forms of economic damage and injury may take years to  
20 detect, and the potential scope can only be assessed after a thorough investigation of the  
21 facts and events surrounding the theft mentioned above.  
22  
23  
24  
25  
26  
27  
28





1 breached is protected and covered by the below data breach statutes.

2           135. Plaintiffs' and Class members' names, social security numbers, phone  
3 numbers, driver's license numbers, birth dates, credit card numbers and email addresses  
4 constitute personal information under and subject to the below state data breach  
5 statutes.  
6

7           136. Equifax unreasonably delayed in informing the public, including Plaintiffs  
8 and members of the Class about the breach of security of Plaintiffs' and Class  
9 members' confidential and non-public personal information after Equifax knew or  
10 should have known that the data breach had occurred.  
11

12           137. Equifax failed to disclose to Plaintiffs and Class members without  
13 unreasonable delay and in the most expedient time possible, the breach of security of  
14 Plaintiffs' and Class members' personal and financial information when Equifax knew  
15 or reasonably believed such information had been compromised.  
16

17           138. Plaintiffs and members of the Class suffered harm directly resulting from  
18 Equifax's failure to provide and the delay in providing Plaintiffs and Class members  
19 with timely and accurate notice as required by the below state data breach statutes.  
20 Plaintiffs suffered the damages alleged above as a direct result of Equifax's delay in  
21 providing timely and accurate notice of the data breach.  
22

23           139. Had Equifax provided timely and accurate notice of the Equifax data  
24 breach, Plaintiffs and Class members would have been able to avoid and/or attempt to  
25 ameliorate or mitigate the damages and harm resulting in the unreasonable delay by  
26  
27  
28

1 Equifax in providing notice. Plaintiffs and Class members could have contacted their  
2 banks to cancel their cards, or could otherwise have tried to avoid the harm caused by  
3  
4 Equifax's delay in providing timely and accurate notice.

5 140. Equifax's failure to provide timely and accurate notice of the Equifax data  
6 breach violated the following state data breach statutes:

- 7 a. Alaska Stat. Ann. § 45.48.010(a), et seq.;
- 8 b. Ark. Code Ann. § 4-110-105(a), et seq.;
- 9 c. Cal. Civ. Code § 1798.83(a), et seq.;
- 10 d. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;
- 11 e. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;
- 12 f. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;
- 13 g. D.C. Code § 28-3852(a), et seq.;
- 14 h. Fla. Stat. Ann. § 501.171(4), et seq.;
- 15 i. Ga. Code Ann. § 10-1-912(a), et seq.;
- 16 j. Haw. Rev. Stat. § 487N-2(a), et seq.;
- 17 k. Idaho Code Ann. § 28-51-105(1), et seq.;
- 18 l. Ill. Comp. Stat. Ann. 530/10(a), et seq.;
- 19 m. Iowa Code Ann. § 715C.2(1), et seq.;
- 20 n. Kan. Stat. Ann. § 50-7a02(a), et seq.;
- 21 o. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;
- 22 p. La. Rev. Stat. Ann. § 51:3074(A), et seq.;

- 1 q. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;
- 2 r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;
- 3 s. Mich. Comp. Laws Ann. § 445.72(1), et seq.;
- 4 t. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;
- 5 u. Mont. Code Ann. § 30-14-1704(1), et seq.;
- 6 v. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;
- 7 w. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;
- 8 x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;
- 9 y. N.J. Stat. Ann. § 56:8-163(a), et seq.;
- 10 z. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;
- 11 aa. N.D. Cent. Code Ann. § 51-30-02, et seq.;
- 12 bb. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;
- 13 cc. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;
- 14 dd. R.I. Gen. Laws Ann. § 11-49.2-3(a), et seq.;
- 15 ee. S.C. Code Ann. § 39-1-90(A), et seq.;
- 16 ff. Tenn. Code Ann. § 47-18-2107(b), et seq.;
- 17 gg. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;
- 18 hh. Utah Code Ann. § 13-44-202(1), et seq.;
- 19 ii. Va. Code. Ann. § 18.2-186.6(B), et seq.;
- 20 jj. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;
- 21 kk. Wis. Stat. Ann. § 134.98(2), et seq.; and
- 22
- 23
- 24
- 25
- 26
- 27
- 28



1 electronic environment in violation of California's data breach statute, Cal. Civ. Code §  
2 1798.81.5, which requires Equifax to take reasonable methods of safeguarding the PII  
3 of Plaintiffs and California Subclass members.  
4

5 145. In addition, Equifax engaged in unlawful acts and practices with respect to  
6 its services by failing to discover and then disclose the data breach to Plaintiffs and  
7 California Subclass members in a timely and accurate manner, contrary to the duties  
8 imposed by Cal. Civ. Code § 1798.82. To date, Equifax has still not provided such  
9 sufficient information to Plaintiffs and the California Subclass members.  
10

11 146. As a direct and proximate result of Equifax's unlawful acts and practices,  
12 Plaintiffs and California Subclass members were injured and lost money or property,  
13 including but not limited to the loss of their legally protected interest in the  
14 confidentiality and privacy of their PII, and additional losses described above.  
15  
16

17 147. Equifax knew or should have known that its system had been breached and  
18 data security practices were inadequate to safeguard California Subclass members' PII  
19 and that the risk of a data breach or theft was highly likely. Equifax's actions in  
20 engaging in the above-named unlawful practices and acts were negligent, knowing and  
21 willful, and/or wanton and reckless with respect to the rights of California Subclass  
22 members.  
23  
24

25 148. Plaintiffs and California Subclass members seek relief under Cal. Bus. &  
26 Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiffs and  
27 California Subclass members of money or property that Equifax may have acquired by  
28

1 means of its unlawful, and unfair business practices, restitutionary disgorgement of all  
2 profits accruing to Equifax because of its unlawful and unfair business practices,  
3  
4 declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5),  
5 and injunctive or other equitable relief.

6  
7 **COUNT VII**  
8 **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW –**  
9 **UNFAIR BUSINESS PRACTICES**  
10 **(ON BEHALF OF PLAINTIFFS AND THE CALIFORNIA SUBCLASS)**

11 149. Plaintiffs reallege and incorporate paragraphs 1 through 74 above.

12 150. This is a statutory claim for relief based on Equifax's violations of the  
13 California Unfair Competition Law, Cal Bus. & Prof. Code § 17200 for Unfair  
14 Business Practices.

15 151. Equifax engaged in unfair acts and practices by soliciting and collecting  
16 Plaintiffs' and California Subclass members' PII with knowledge that the information  
17 would not be adequately protected; while Plaintiffs' and California Subclass members'  
18 PII would be processed in an unsecure electronic environment. These unfair acts and  
19 practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or  
20 substantially injurious to Plaintiffs and California Subclass members. They were likely  
21 to deceive the public into believing their PII was secure, when it was not. The harm  
22 these practices caused to Plaintiffs and California Subclass members outweighed their  
23 utility, if any.

24 152. Equifax engaged in unfair acts and practices with respect to the provision  
25  
26  
27  
28

1 of its services by failing to enact adequate privacy and security measures and protect  
2 California Subclass members' PII from further unauthorized disclosure, release, data  
3 breaches, and theft, and failing to timely discovery and give notice of the Data Breach.  
4 These unfair acts and practices were immoral, unethical, oppressive, unscrupulous,  
5 unconscionable, and/or substantially injurious to Plaintiffs and California Subclass  
6 members. They were likely to deceive the public into believing their PII was secure,  
7 when it was not. The harm these practices caused to Plaintiffs and California Subclass  
8 members outweighed their utility, if any.  
9  
10

11  
12 153. As a direct and proximate result of Equifax's acts of unfair practices and  
13 acts, Plaintiffs and California Subclass members were injured and lost money or  
14 property, including but not limited to the loss of their legally protected interest in the  
15 confidentiality and privacy of their PII, and additional losses described above.  
16

17 154. Equifax knew or should have known that its systems and data security  
18 practices were inadequate to safeguard California Subclass members' PII and that the  
19 risk of a data breach or theft was highly likely. Equifax's actions in engaging in the  
20 above-named unlawful practices and acts were negligent, knowing and willful, and/or  
21 wanton and reckless with respect to the rights of California Subclass members.  
22  
23

24 155. The Plaintiffs and California Subclass members seek relief under Cal. Bus.  
25 & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution of money or  
26 property that Equifax may have acquired by means of its unfair business practices,  
27 restitutionary disgorgement of all profits accruing to Equifax because of its unfair  
28

1 business practices, declaratory relief, attorney’s fees and costs (pursuant to Cal. Code  
2 Civ. Proc. §1021.5), and injunctive or other equitable relief.

3  
4 **COUNT VIII**  
5 **VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW –**  
6 **FRAUDULENT/DECEPTIVE BUSINESS PRACTICES**  
7 **(ON BEHALF OF PLAINTIFFS AND THE CALIFORNIA SUBCLASS)**

8 156. Plaintiffs reallege and incorporate paragraphs 1 through 74 above.

9 157. This is a statutory claim for relief based on Equifax’s violations of the  
10 California Unfair Competition Law, Cal Bus. & Prof. Code § 17200 for  
11 Fraudulent/Deceptive Business Practices.

12 158. Equifax has violated Cal. Bus. and Prof. Code §17200 et seq. by engaging  
13 in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive,  
14 untrue or misleading advertising that constitute acts of “unfair competition” as defined  
15 in Cal. Bus. Prof. Code §17200. Equifax engaged in unlawful acts and practices with  
16 respect to its services by establishing the sub-standard security practices and procedures  
17 described herein; by soliciting and collecting Plaintiffs’ and California Subclass  
18 members’ PII with knowledge that the information would not be adequately protected;  
19 and by gathering Plaintiffs’ and California Subclass members’ PII in an unsecure  
20 electronic environment in violation of California’s data breach statute, Cal. Civ. Code §  
21 1798.81.5, which requires Equifax to take reasonable methods of safeguarding the PII  
22 of Plaintiffs and the California Subclass Members.

23 159. In addition, Equifax engaged in unlawful acts and practices with respect to  
24 its services by failing to discover and then disclose the data breach to Plaintiffs and  
25 California Subclass members in a timely and accurate manner, contrary to the duties  
26 imposed by Cal. Civ. Code § 1798.82. To date, Equifax has still not provided such  
27 sufficient information to Plaintiffs and the California Subclass members.  
28



1 165. Equifax still possesses PII pertaining to Plaintiffs and Class members.

2 166. Equifax has made no announcement or notification that it has remedied the  
3  
4 vulnerabilities in its computer data systems, and, most importantly, its systems.

5 167. Accordingly, Equifax has not satisfied its contractual obligations and legal  
6  
7 duties to Plaintiffs and Class members. In fact, now that Equifax's lax approach  
8  
9 towards data security has become public, the PII in its possession is more vulnerable  
10  
11 than previously.

12 168. Actual harm has arisen in the wake of the Equifax Data Breach regarding  
13  
14 Equifax's contractual obligations and duties of care to provide data security measures to  
15  
16 Plaintiffs and Class members.

17 169. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data  
18  
19 security measures do not comply with its contractual obligations and duties of care, and  
20  
21 (b) in order to comply with its contractual obligations and duties of care, Equifax must  
22  
23 implement and maintain reasonable security measures, including, but not limited to:

- 24 a. Engaging third-party security auditors/penetration testers as well as  
25 internal security personnel to conduct testing, including simulated  
26 attacks, penetration tests, and audits on Equifax's systems on a  
27 periodic basis, and ordering Equifax to promptly correct any  
28 problems or issues detected by such third-party security auditors;
- 29 b. Engaging third-party security auditors and internal personnel to run  
30 automated security monitoring;
- 31 c. Auditing, testing, and training its security personnel regarding any  
32 new or modified procedures;
- 33 d. Segmenting PII by, among other things, creating firewalls and  
34 access controls so that if one area of Equifax is compromised,

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

- hackers cannot gain access to other portions of Equifax systems;
- e. Purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;
- f. Conducting regular database scanning and securing checks;
- g. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. Educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

**REQUEST FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against EQUIFAX as follows:

- a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and her Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes or California Subclass;
- b. For an Order finding that Equifax breached its duty to safeguard and protect the PII and financial information of Plaintiffs and members of the Classes that was compromised in the Data Breach;
- c. For an award of damages, as allowed by law in an amount to be determined;



**JURY TRIAL DEMAND**

Plaintiff demands a jury trial on all issues so triable as a matter of right.

Dated: November 1, 2017

GIRARDI & KEESE

By: /s/ Christopher T. Aumais

Thomas V. Girardi  
California Bar No. 36603  
Robert W. Finnerty  
California Bar No. 119775  
Christopher T. Aumais  
California Bar No. 249901  
1126 Wilshire Boulevard  
Los Angeles, California 90017  
Telephone: (213) 977-0211  
Facsimile: (213) 481-1554  
Email: [tgirardi@girardikeese.com](mailto:tgirardi@girardikeese.com)  
Email: [rfinnerty@girardikeese.com](mailto:rfinnerty@girardikeese.com)  
Email: [caumais@girardikeese.com](mailto:caumais@girardikeese.com)

RUSSOMANNO & BORRELLO, P.A.

By: /s/ Herman J. Russomanno

Museum Tower – Penthouse 2800  
150 West Flagler Street  
Miami, Florida 33130  
Telephone: (305) 373-2101  
Facsimile: (305) 373-2103  
Herman J. Russomanno (Fla. Bar No. 240346)  
[hrussomanno@russomanno.com](mailto:hrussomanno@russomanno.com)  
Robert J. Borrello (Fla Bar No 764485)  
[rborrello@russomanno.com](mailto:rborrello@russomanno.com)  
Herman J. Russomanno III (FlaBarNo. 21249)  
[herman2@russomanno.com](mailto:herman2@russomanno.com)

Edward G. Rubinoff  
Fla. Bar No. 97785  
Andrew Moss  
Florida Bar No. 0170259  
Motion for PHV Admission to Be Filed  
KUTNER, RUBINOFF & MOSS  
2665 S. Bayshore Drive, Ste. 30 I  
Coconut Grove, FL 33133  
Tel: 305-358-6200  
Fax: 305-577-8230  
Email: [rubinoff@krmlegal.com](mailto:rubinoff@krmlegal.com)  
Email: [moss@krmlegal.com](mailto:moss@krmlegal.com)

David A. Nunez  
Fla. Bar No. 646776  
Motion for PHV Admission to Be Filed  
MEYER & NUNEZ, P.A.  
150 W. Flagler Street, Ste. 2700  
Miami, FL 33130  
Tel: 305-722-9898  
Fax: 305-3 71-9197  
Email: [david@nunez-law.com](mailto:david@nunez-law.com)

**Attorneys for Plaintiff and the Classes**

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET

**I. (a) PLAINTIFFS** ( Check box if you are representing yourself  )  
Amanda Janaye White, and Robert Honanian, individually and on behalf of all others similarly situated

**DEFENDANTS** ( Check box if you are representing yourself  )  
EQUIFAX, INC., a Georgia corporation

(b) County of Residence of First Listed Plaintiff Riverside  
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant \_\_\_\_\_  
(IN U.S. PLAINTIFF CASES ONLY)

(c) Attorneys (Firm Name, Address and Telephone Number) If you are representing yourself, provide the same information.  
Thomas V. Girardi, SBN: 36603  
Robert W. Finnerty, SBN: 119775  
Christopher T. Aumais, SBN: 249901  
GIRARDI | KEESE, 1126 Wilshire Blvd., L.A. 213-977-0211

Attorneys (Firm Name, Address and Telephone Number) If you are representing yourself, provide the same information.

**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**-For Diversity Cases Only  
(Place an X in one box for plaintiff and one for defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	<input type="checkbox"/> 4	<input type="checkbox"/> 4
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

**IV. 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

**V. REQUESTED IN COMPLAINT: JURY DEMAND:**  Yes  No (Check "Yes" only if demanded in complaint.)

**CLASS ACTION under F.R.Cv.P. 23:**  Yes  No **MONEY DEMANDED IN COMPLAINT:** \$ 10,000,000.

**VI. CAUSE OF ACTION** (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)  
COA: WILLFUL VIOLATION OF FAIR CREDIT REPORTING ACT

**VII. NATURE OF SUIT** (Place an X in one box only).

OTHER STATUTES	CONTRACT	REAL PROPERTY CONT.	IMMIGRATION	PRISONER PETITIONS	PROPERTY RIGHTS
<input type="checkbox"/> 375 False Claims Act	<input type="checkbox"/> 110 Insurance	<input type="checkbox"/> 240 Torts to Land	<input type="checkbox"/> 462 Naturalization Application	<b>Habeas Corpus:</b>	<input type="checkbox"/> 820 Copyrights
<input type="checkbox"/> 376 Qui Tam (31 USC 3729(a))	<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 463 Alien Detainee	<input type="checkbox"/> 830 Patent
<input type="checkbox"/> 400 State Reapportionment	<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 290 All Other Real Property	<b>TORTS</b>	<input type="checkbox"/> 510 Motions to Vacate Sentence	<input type="checkbox"/> 840 Trademark
<input type="checkbox"/> 410 Antitrust	<input type="checkbox"/> 140 Negotiable Instrument	<b>TORTS</b>	<b>PERSONAL PROPERTY</b>	<input type="checkbox"/> 530 General	<b>SOCIAL SECURITY</b>
<input type="checkbox"/> 430 Banks and Banking	<input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment	<b>PERSONAL INJURY</b>	<input type="checkbox"/> 370 Other Fraud	<input type="checkbox"/> 535 Death Penalty	<input type="checkbox"/> 861 HIA (1395ff)
<input type="checkbox"/> 450 Commerce/ICC Rates/Etc.	<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 371 Truth in Lending	<b>Other:</b>	<input type="checkbox"/> 862 Black Lung (923)
<input type="checkbox"/> 460 Deportation	<input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Vet.)	<input type="checkbox"/> 315 Airplane Product Liability	<input type="checkbox"/> 380 Other Personal Property Damage	<input type="checkbox"/> 540 Mandamus/Other	<input type="checkbox"/> 863 DIWC/DIWW (405 (g))
<input type="checkbox"/> 470 Racketeer Influenced & Corrupt Org.	<input type="checkbox"/> 153 Recovery of Overpayment of Vet. Benefits	<input type="checkbox"/> 320 Assault, Libel & Slander	<input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 550 Civil Rights	<input type="checkbox"/> 864 SSID Title XVI
<input checked="" type="checkbox"/> 480 Consumer Credit	<input type="checkbox"/> 160 Stockholders' Suits	<input type="checkbox"/> 330 Fed. Employers' Liability	<b>BANKRUPTCY</b>	<input type="checkbox"/> 555 Prison Condition	<input type="checkbox"/> 865 RSI (405 (g))
<input type="checkbox"/> 490 Cable/Sat TV	<input type="checkbox"/> 190 Other Contract	<input type="checkbox"/> 340 Marine	<input type="checkbox"/> 422 Appeal 28 USC 158	<b>FORFEITURE/PENALTY</b>	<b>FEDERAL TAX SUITS</b>
<input type="checkbox"/> 850 Securities/Commodities/Exchange	<input type="checkbox"/> 195 Contract Product Liability	<input type="checkbox"/> 345 Marine Product Liability	<input type="checkbox"/> 423 Withdrawal 28 USC 157	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)
<input type="checkbox"/> 890 Other Statutory Actions	<input type="checkbox"/> 196 Franchise	<input type="checkbox"/> 350 Motor Vehicle	<b>CIVIL RIGHTS</b>	<input type="checkbox"/> 690 Other	<input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
<input type="checkbox"/> 891 Agricultural Acts	<b>REAL PROPERTY</b>	<input type="checkbox"/> 355 Motor Vehicle Product Liability	<input type="checkbox"/> 440 Other Civil Rights	<b>LABOR</b>	
<input type="checkbox"/> 893 Environmental Matters	<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 441 Voting	<input type="checkbox"/> 710 Fair Labor Standards Act	
<input type="checkbox"/> 895 Freedom of Info. Act	<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 362 Personal Injury-Med Malpractice	<input type="checkbox"/> 442 Employment	<input type="checkbox"/> 720 Labor/Mgmt. Relations	
<input type="checkbox"/> 896 Arbitration	<input type="checkbox"/> 230 Rent Lease & Ejectment	<input type="checkbox"/> 365 Personal Injury-Product Liability	<input type="checkbox"/> 443 Housing/Accommodations	<input type="checkbox"/> 740 Railway Labor Act	
<input type="checkbox"/> 899 Admin. Procedures Act/Review of Appeal of Agency Decision		<input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability	<input type="checkbox"/> 445 American with Disabilities-Employment	<input type="checkbox"/> 751 Family and Medical Leave Act	
<input type="checkbox"/> 950 Constitutionality of State Statutes		<input type="checkbox"/> 368 Asbestos Personal Injury Product Liability	<input type="checkbox"/> 446 American with Disabilities-Other	<input type="checkbox"/> 790 Other Labor Litigation	
			<input type="checkbox"/> 448 Education	<input type="checkbox"/> 791 Employee Ret. Inc. Security Act	

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**

**VIII. VENUE:** Your answers to the questions below will determine the division of the Court to which this case will be initially assigned. This initial assignment is subject to change, in accordance with the Court's General Orders, upon review by the Court of your Complaint or Notice of Removal.

<b>QUESTION A: Was this case removed from state court?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "no," skip to Question B. If "yes," check the box to the right that applies, enter the corresponding division in response to Question E, below, and continue from there.	STATE CASE WAS PENDING IN THE COUNTY OF:	INITIAL DIVISION IN CACD IS:
	<input type="checkbox"/> Los Angeles, Ventura, Santa Barbara, or San Luis Obispo	Western
	<input type="checkbox"/> Orange	Southern
	<input type="checkbox"/> Riverside or San Bernardino	Eastern

<b>QUESTION B: Is the United States, or one of its agencies or employees, a PLAINTIFF in this action?</b>  <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "no," skip to Question C. If "yes," answer Question B.1, at right.	<b>B.1. Do 50% or more of the defendants who reside in the district reside in Orange Co.?</b>  check one of the boxes to the right →	YES. Your case will initially be assigned to the Southern Division. <input type="checkbox"/> Enter "Southern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Continue to Question B.2.
	<b>B.2. Do 50% or more of the defendants who reside in the district reside in Riverside and/or San Bernardino Counties? (Consider the two counties together.)</b>  check one of the boxes to the right →	YES. Your case will initially be assigned to the Eastern Division. <input type="checkbox"/> Enter "Eastern" in response to Question E, below, and continue from there.  NO. Your case will initially be assigned to the Western Division. <input type="checkbox"/> Enter "Western" in response to Question E, below, and continue from there.

<b>QUESTION C: Is the United States, or one of its agencies or employees, a DEFENDANT in this action?</b>  <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "no," skip to Question D. If "yes," answer Question C.1, at right.	<b>C.1. Do 50% or more of the plaintiffs who reside in the district reside in Orange Co.?</b>  check one of the boxes to the right →	YES. Your case will initially be assigned to the Southern Division. <input type="checkbox"/> Enter "Southern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Continue to Question C.2.
	<b>C.2. Do 50% or more of the plaintiffs who reside in the district reside in Riverside and/or San Bernardino Counties? (Consider the two counties together.)</b>  check one of the boxes to the right →	YES. Your case will initially be assigned to the Eastern Division. <input type="checkbox"/> Enter "Eastern" in response to Question E, below, and continue from there.  NO. Your case will initially be assigned to the Western Division. <input type="checkbox"/> Enter "Western" in response to Question E, below, and continue from there.

<b>QUESTION D: Location of plaintiffs and defendants?</b>	<b>A.</b> Orange County	<b>B.</b> Riverside or San Bernardino County	<b>C.</b> Los Angeles, Ventura, Santa Barbara, or San Luis Obispo County
Indicate the location(s) in which 50% or more of <i>plaintiffs who reside in this district</i> reside. (Check up to two boxes, or leave blank if none of these choices apply.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Indicate the location(s) in which 50% or more of <i>defendants who reside in this district</i> reside. (Check up to two boxes, or leave blank if none of these choices apply.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<b>D.1. Is there at least one answer in Column A?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "yes," your case will initially be assigned to the SOUTHERN DIVISION. Enter "Southern" in response to Question E, below, and continue from there.  If "no," go to question D2 to the right. →	<b>D.2. Is there at least one answer in Column B?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  If "yes," your case will initially be assigned to the EASTERN DIVISION. Enter "Eastern" in response to Question E, below.  If "no," your case will be assigned to the WESTERN DIVISION. Enter "Western" in response to Question E, below. ↓
---	---

<b>QUESTION E: Initial Division?</b>	INITIAL DIVISION IN CACD
Enter the initial division determined by Question A, B, C, or D above: →	Western

<b>QUESTION F: Northern Counties?</b>
Do 50% or more of plaintiffs or defendants in this district reside in Ventura, Santa Barbara, or San Luis Obispo counties? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**

**IX(a). IDENTICAL CASES:** Has this action been previously filed in this court?  NO  YES

If yes, list case number(s): \_\_\_\_\_

**IX(b). RELATED CASES:** Is this case related (as defined below) to any civil or criminal case(s) previously filed in this court?  NO  YES

If yes, list case number(s): \_\_\_\_\_

**Civil cases** are related when they (check all that apply):

- A. Arise from the same or a closely related transaction, happening, or event;
- B. Call for determination of the same or substantially related or similar questions of law and fact; or
- C. For other reasons would entail substantial duplication of labor if heard by different judges.

Note: That cases may involve the same patent, trademark, or copyright is not, in itself, sufficient to deem cases related.

**A civil forfeiture case and a criminal case** are related when they (check all that apply):

- A. Arise from the same or a closely related transaction, happening, or event;
- B. Call for determination of the same or substantially related or similar questions of law and fact; or
- C. Involve one or more defendants from the criminal case in common and would entail substantial duplication of labor if heard by different judges.

**X. SIGNATURE OF ATTORNEY (OR SELF-REPRESENTED LITIGANT):** \_\_\_\_\_ DATE: November 1, 2017

*Christopher T. Dumais*

**Notice to Counsel/Parties:** The submission of this Civil Cover Sheet is required by Local Rule 3-1. This Form CV-71 and the information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. For more detailed instructions, see separate instruction sheet (CV-071A).

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405 (g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405 (g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405 (g))