

1 R. Alexander Saveri (SBN 173102)
 Geoffrey C. Rushing (SBN 126910)
 2 Cadio Zirpoli (SBN 179108)
 Sarah Van Culin (SBN 293181)
 3 SAVERI & SAVERI, INC.
 706 Sansome Street
 4 San Francisco, CA 94111
 Telephone: (415) 217-6810
 5 Facsimile: (415) 217-6813
 6 Email: rick@saveri.com; geoff@saveri.com;
cadio@saveri.com; sarah@saveri.com
 7

8 Randall Robinson Renick (SBN 179652)
 HADSELL STORMER RICHARDSON & RENICK, LLP
 9 128 N. Fair Oaks Ave.
 Pasadena, CA 91103
 10 Telephone: (626) 585-9600
 11 Facsimile: (626) 577-7079
 Email: rrr@hadsellstormer.com

12 *Counsel for Plaintiff*

13
 14 **UNITED STATES DISTRICT COURT**
 15 **NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION**
 16

17 MICHAEL BRANCH, Individually and on
 18 Behalf of All Others Similarly Situated,

19 Plaintiffs,

20 vs.

21 EQUIFAX, INC.

22 Defendant.

CASE NO.: 3:17-cv-05429

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff, Michael Branch, individually and on behalf of all those similarly situated,
2 brings this action for damages and equitable relief against Equifax, Inc. and alleges, based upon
3 the investigation of counsel and on information and belief, as follows:

4 **I. OVERVIEW**

5 1. On September 7, 2017, Equifax, Inc. (“Equifax” or “Defendant”) announced the
6 largest data breach in history. Hackers used a known vulnerability in an Equifax website
7 application to gain access to confidential personal information including names, Social Security
8 numbers, addresses, birth dates, and, in some instances, driver’s license numbers of some 143
9 million Americans.

10 2. After discovering the hack on July 29, 2017, Equifax waited 40 days to make
11 news of the data breach public, leaving consumers at heightened risk of identity theft for over a
12 month.

13 3. The hackers were able to gain access to this confidential personal information by
14 exploiting a known Apache Struts vulnerability that had been publicized—and a patch issued—
15 two months before the hack occurred.

16 4. Equifax’s negligence in failing to repair this known vulnerability and its failure to
17 take reasonable security measures to protect consumer data means millions of Americans are
18 now at risk of identity theft and have incurred expenses and inconvenience in addressing the
19 consequences of this data breach.

20 5. Plaintiff and members of the proposed Classes have suffered harm and face the
21 imminent risk of future harm, including:

22 a. Costs associated with the detection and prevention of identity theft and
23 unauthorized use of their confidential personal information;

24 b. Costs incurred in and the loss of productivity from taking time to address,
25 mitigate, and deal with the actual and future consequences of this data breach, including finding
26 and challenging fraudulent changes to debit and credit accounts, cancelling credit cards,
27

1 imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance,
2 and annoyance of dealing with all of the issues resulting from this data breach;

3 c. Theft of their personal information;

4 d. Imminent, impending threat of fraud and identity theft as a result of their
5 personal information being in the hands of hackers and already misused and sold on the Internet
6 and/or black market;

7 e. Loss of use of and access to their account funds and costs associated with
8 their inability to obtain money from their accounts or being limited in the amount of money they
9 could obtain from their accounts, including missing payments on bills and loans, late charges and
10 fees, and adverse effects on credit including decreased credit scores and adverse credit notations;

11 f. Damage to and the diminution in value of confidential personal
12 information entrusted to Equifax for the sole purpose of reporting and/or monitoring their credit
13 profile with the mutual understanding that Equifax would safeguard Plaintiff and the Class
14 members' data against theft and not allow access and misuse of their data by others;

15 g. Any money paid for products purchased from Equifax (such as credit
16 monitoring or credit score inquiries) at any time after July 29, 2017 when the data breach was
17 discovered by Equifax because they would not have engaged Equifax for those services if
18 Equifax had disclosed that it lacked adequate systems and procedures to reasonably safeguard
19 customers' confidential personal information; and

20 h. Continued risk to their confidential personal information that is still in
21 Equifax's possession and which is at risk of further breaches so long as Equifax fails to
22 undertake adequate measures to protect the data.

23 6. Plaintiff brings this action on behalf of himself individually and all those similarly
24 situated in order to redress the harm already suffered by the class and to prevent future failures
25 by Equifax to protect consumer data. Plaintiff seeks damages and equitable relief.

26 **II. PARTIES**

27 7. Plaintiff, Michael Branch, is a resident of Los Angeles County, California, whose
28

1 confidential personal information was included in the data breach of Equifax’s systems and
2 disclosed to unauthorized third parties and Mr. Branch was harmed as a direct and proximate
3 result of the conduct alleged herein. Mr. Branch entered his last name and the last six digits of
4 his social security number into the Equifaxsecurity2017.com “Check Potential Impact” webpage
5 and was informed that his confidential personal information may have been impacted by the data
6 breach.

7 8. Defendant, Equifax, Inc., is a Georgia corporation with its headquarters in
8 Atlanta, Georgia. Equifax, Inc. is registered with the California Secretary of State’s office as an
9 Active Foreign Stock Corporation. Equifax conducts business throughout the United States,
10 including in the Northern District of California, and did so during the Class Period.

11 9. Equifax has offices in California including in Moorpark, near Los Angeles.
12 TrustedID, Inc., is owned by Equifax and is a Delaware Corporation with its principal office in
13 Palo Alto, California.

14 **III. JURISDICTION AND VENUE**

15 10. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §
16 1332(d)(2) because the matter in controversy exceeds \$5 million, exclusive of interest and costs,
17 and at least one plaintiff and the defendant are citizens of different states. There are more than
18 100 putative class members.

19 11. This Court has jurisdiction over Equifax because Equifax is authorized to and
20 regularly does conduct business in California and has sufficient minimum contacts with
21 California. Equifax transacted business throughout the United States, including in this District;
22 sold or marketed its products throughout the United States, including in this District; and
23 purposefully availed itself of the laws of the United States and the State of California. Equifax
24 reported to the Office of the Attorney General for the State of California that approximately
25 15,178,887 California residents were potentially impacted by the data breach.

26 12. Venue is proper in this District because Equifax is licensed to do business in and
27 is doing business in this District, the Court has personal jurisdiction over Equifax, and because a
28

1 substantial part of the events giving rise to the claim occurred in this District.

2 13. This action is not subject to arbitration. Equifax’s website states:

3 [E]nrolling in the free credit file monitoring and identity theft protection that we
4 are offering as part of this cybersecurity incident does not waive any rights to take
5 legal action. We removed that language from the Terms of Use on the website,
6 www.equifaxsecurity2017.com. The Terms of Use on www.equifax.com do not
apply to the TrustedID Premier product being offered to consumers as a result of
the cybersecurity incident.¹

7 **IV. FACTUAL ALLEGATIONS**

8 14. There are three major credit reporting agencies in the United States—Equifax,
9 Experian, and TransUnion.² These agencies are responsible for running the reports that are used
10 to calculate consumers’ credit scores; impacting their ability to get a mortgage, buy a car, or
11 engage in any number of other financial transactions.³

12 15. Private information is Equifax’s lifeblood. Equifax organizes and analyzes data
13 on more than 820 million consumers and more than 91 million businesses worldwide. Its
14 database includes employee data contributed from more than 7,100 employers.⁴ Equifax operates
15 or has investments in 24 countries spanning North America, Central and South America, Europe
16 and the Asia Pacific region.⁵ Last year, Equifax made \$3.1 billion in revenue.⁶

17 16. Equifax is well aware of the private, sensitive nature of the information it stores.
18 The Equifax website describes identity theft as “when someone steals your personal information
19 – such as your name, Social Security number, and date of birth – typically to hijack your credit
20 and use it to open up new credit accounts, take out loans in your name, or access your bank or
21 retirement accounts.”⁷ The Equifax website also describes how this stolen information is used:

22
23
24 ¹ <https://www.equifaxsecurity2017.com/2017/09/11/progress-update-consumers-2/> [A Progress
Update for Consumers, September 11, 2017]

25 ² <https://www.nytimes.com/2017/09/08/business/equifax.html>

26 ³ <https://www.nytimes.com/2017/09/08/business/equifax.html>

27 ⁴ <http://www.equifax.com/about-equifax>

28 ⁵ <http://www.equifax.com/about-equifax>

⁶ <https://www.nytimes.com/2017/09/08/business/equifax.html>

⁷ <https://www.equifax.com/personal/education/identity-theft/what-is-identity-theft>

1 An identity thief can even use your personal information to steal your tax refunds,
2 seek medical services, or commit crimes in your name. Once an identity thief has
access to your personal information, he or she can also:

3 Open new credit card accounts with your name, Social Security number and date
4 of birth. When the thief charges to the credit cards and leaves the bills unpaid, the
5 delinquency will be reported to your credit report and could impact your credit
score;

6 Open a bank account in your name and write bad checks on the account;

7 Create counterfeit checks or debit cards and use them to drain your existing bank
8 accounts;

9 File for bankruptcy under your name to avoid paying debts;

10 Set up a phone, wireless, or other utility service in your name.⁸

11 17. After outlining this parade of horrors for consumers, Equifax suggests
12 consumers “Consider these Products” including “Equifax ID Patrol™,” “Equifax ID Patrol™
13 Premier” and “Equifax Complete™ Advantage Plan” that claim to help consumers monitor their
14 credit and protect their identity.

15 18. The Equifax data breach is one of the largest breaches ever.⁹ From mid-May
16 through July 2017, “Criminals exploited a U.S. website application vulnerability to gain access
17 to certain files” held by Equifax.¹⁰ These files contained the names, Social Security numbers,
18 birth dates, and addresses and, in some instances, driver’s license numbers of some 143 million
19 U.S. consumers.¹¹ In addition, the credit card numbers for approximately 209,000 U.S.
20 consumers, and certain dispute documents with the personal identifying information for
21 approximately 182,000 U.S. consumers were accessed.¹² Equifax also identified unauthorized
22 access to limited personal information for certain UK and Canadian residents.¹³

23
24
25 ⁸ <https://www.equifax.com/personal/education/identity-theft/what-is-identity-theft>

26 ⁹ <http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX>

27 ¹⁰ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

28 ¹¹ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

¹² <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

¹³ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

1 19. Approximately 15,178,887 California residents were potentially affected by this
2 data breach.¹⁴

3 20. Equifax has stated that this breach was due to an Apache Struts vulnerability:
4 “The vulnerability was Apache Struts CVE-2017-5638.”¹⁵

5 21. The vulnerability identified by Equifax as the cause of this data breach had been
6 discovered and patched some two months before the data breach.¹⁶ Equifax did not update its
7 website applications to fix this issue, despite reports back in March that hackers were actively
8 targeting this vulnerability.¹⁷ Instead Equifax’s website indicates that patching of this
9 vulnerability did not occur until late July, after the breach had occurred:

10 On July 29, 2017, Equifax’s Security team observed suspicious network traffic
11 associated with its U.S. online dispute portal web application. In response, the
12 Security team investigated and blocked the suspicious traffic that was identified.

13 The Security team continued to monitor network traffic and observed additional
14 suspicious activity on July 30, 2017. In response, the company took offline the
15 affected web application that day.

16 The company’s internal review of the incident continued. Upon discovering a
17 vulnerability in the Apache Struts web application framework as the initial attack
18 vector, Equifax patched the affected web application before bringing it back
19 online.¹⁸

20 22. “Apache Struts is free, open-source software used to create Java web
21 applications.”¹⁹ However, as noted by Boris Chen, vice president of engineering at tCell in an
22 interview with USA Today: “A single vulnerability in a web component should not result in
23 millions of highly sensitive records being exfiltrated. Security controls should have existed at

24 ¹⁴ [https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-
25 following-equifax-data-breach](https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach); [https://oag.ca.gov/system/files/Equifax%20-
26 %20CA%20Letter_0.pdf](https://oag.ca.gov/system/files/Equifax%20-%20CA%20Letter_0.pdf)

27 ¹⁵ <https://www.equifaxsecurity2017.com/2017/09/13/progress-update-consumers-4/>

28 ¹⁶ [https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-
failure-to-patch-two-month-old-bug/](https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/)

¹⁷ [https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-
attack-imperils-high-impact-sites/](https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/)

¹⁸ <https://www.equifaxsecurity2017.com/> [Consumer Update, September 15, 2017]

¹⁹ [https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-
answers-and-some-questions/658343001/](https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/)

1 many points along the way to stop such a catastrophic outcome.”²⁰

2 23. Equifax discovered the data breach on July 29, 2017 but did not make this
3 information public until September 7, 2017, some 40 days later, when Equifax issued a press
4 release.²¹

5 24. While the public was kept in the dark about this massive breach, Equifax
6 executives apparently were not. Three senior executives “sold \$1.8 million worth of shares in the
7 days after Equifax discovered the breach.”²² Equifax shares have dropped 32 percent since the
8 company disclosed the breach.²³

9 25. Equifax knew or should have known that its systems were at-risk of hacking
10 attacks based on previous attacks and reports that its internal system had weaknesses. Equifax
11 failed to improve its data security after two data breaches that occurred in the last year: one in
12 which hackers took valuable W-2 tax and salary data from the Equifax website and, in another,
13 hackers took W-2 tax data from an Equifax subsidiary called TALX. Cybersecurity professionals
14 interviewed by the New York Times concluded that there should have been more controls in
15 place to prevent the most recent data breach, especially in light of these prior incidents.

16 26. The first Equifax security breach, which led to a class action lawsuit, stemmed
17 from a May 2016 incident in which Equifax’s W-2 Express website was breached, leading to the
18 leak of 430,000 names, addresses, social security numbers, and other information. Equifax had
19 clients’ employees access their data with default PIN numbers made up of the last four digits of
20 their social security number and four digit year of birth; assigned PIN numbers that were
21 exceedingly easy for criminals to find on the internet. Equifax agreed to fix the underlying issue
22 that led to this data breach, although it is unclear if the vulnerability has yet to be adequately
23 addressed.

24
25 ²⁰ <https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/>

26 ²¹ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

27 ²² <https://www.nytimes.com/2017/09/08/business/equifax.html>

28 ²³ <http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX>

1 27. The second prior Equifax data breach involving TALX was especially alarming
2 because Equifax failed to discover that breach for almost a year—from April 17, 2016 through
3 March 29, 2017. This breach was not publicly disclosed until May 2017. That security breach
4 related to hackers using personal information to guess client customer questions and ultimately
5 reset their 4-digit PIN to gain access to customers’ tax data.

6 28. Equifax also suffered smaller data breaches in January 2017 concerning LifeLock
7 customer credit information, and a 2013-2014 breach of credit reports using personal
8 information. In 2016, a vulnerability to cross-site scripting was discovered. Cross-site scripting,
9 also known as XSS, is a process by which an attacker could send a link they create to users who
10 would click on the link and long on to the website, revealing their user names and passwords and
11 jeopardizing their personal information.

12 29. Security experts Kenneth White and Kevin Beaumont found that Equifax may
13 have been susceptible to attacks because it uses old and discontinued technologies, like
14 Netscape, IBM Websphere, Apache Struts, and Java. The vulnerabilities of those programs
15 should have been addressed sooner given the sensitivity of information and the risk. AlienVault
16 security advocate, Javvad Malik notes that “[c]ompanies like Equifax should know very well that
17 data is the lifeblood of the organization and its crown jewels.”

18 30. There are several governmental investigations already underway. The FTC has
19 confirmed that they are investigating the Equifax data breach.²⁴ The Consumer Financial
20 Protection Bureau is also investigating Equifax. The chairmen of the House Committee on
21 Science, Space, and Technology and the House Committee on Oversight and Government
22 Reform have said that their respective committees will investigate the Equifax data breach and
23 have requested that Equifax produce documents by September 28.²⁵ Equifax CEO Richard Smith
24 is scheduled to appear at a hearing on the House Subcommittee on Digital Commerce and

25 _____
26 ²⁴ <http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX>; <https://www.usatoday.com/story/money/2017/09/14/ftc-investigating-equifax-over-data-breach/665550001/>

27 ²⁵ <http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX>
28

1 Consumer Protection on October 3.²⁶ The Federal Bureau of Investigation has opened an
2 investigation into the breach, along with nearly 40 states.²⁷

3 31. The FTC website suggests that people consider freezing their credit reports in
4 light of this data breach, but this can be inconvenient in that it keeps consumers from opening
5 new accounts unless they unfreeze them days in advance.

6 32. Further, even if consumers freeze their credit reports with Equifax, they must also
7 freeze them for Experian and TransUnion as well to give them the best protection.

8 33. To add cost to this inconvenience of freezing credit reports, in some states these
9 companies require consumers to pay a fee to freeze and unfreeze their credit reports.

10 34. Unfortunately, even if consumers freeze their credit reports, they are not protected
11 from fraudulent tax returns being filed with their information or people using their credit cards.

12 35. Security analyst at Gartner, Avivah Litan is quoted in a USA Today article as
13 saying that instead of checking credit card statements monthly, people need to now check them
14 weekly and be hyper-vigilant if their information has been jeopardized. This is a further
15 inconvenience that those attached by this data breach must endure.

16 36. In addition to common fears relating to identity theft like credit card use, people
17 opening accounts in another person's name, and harm to a credit score, consequences like
18 medical identity theft (fake IDs used to pay for procedures and surgeries), tax fraud (filing false
19 tax returns to profit from refunds), and synthetic identity theft (combining information from
20 multiple victims to create a new identity) are also possible because of the depth of information
21 stolen.

22 **V. CLASS ALLEGATIONS**

23 37. Plaintiff brings this class action pursuant to Federal Rules of Civil Procedure
24 23(a) and 23(b)(2) and (b)(3) on his own behalf and as representative of the following classes of
25

26 ²⁶ <http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX>; <https://www.usatoday.com/story/money/2017/09/14/ftc-investigating-equifax-over-data-breach/665550001/>

27 ²⁷ <http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX>
28

1 persons and entities (the “Classes”).

2 38. A nationwide “Negligence Class” seeking damages, equitable and injunctive
3 relief:

4 All persons and entities in the United States whose confidential personal
5 information was compromised as a result of the data breach publically announced
6 by Equifax on September 7, 2017. Excluded from the Class is Defendant, its
7 parent companies, subsidiaries and affiliates, employees of Defendant, including
8 its officers and directors; and any judge or jurors assigned to this case.

8 And a “California Class” seeking damages, equitable and injunctive relief:

9 All residents of the State of California whose confidential personal information
10 was compromised as a result of the data breach publically announced by Equifax
11 on September 7, 2017. Excluded from the Class is Defendant, its parent
12 companies, subsidiaries and affiliates, employees of Defendant, including its
13 officers and directors; and any judge or jurors assigned to this case.

13 39. The proposed classes are each so large that joinder of all members is
14 impracticable. Class members are also dispersed geographically, both throughout California and
15 the U.S. While Plaintiff does not know the exact number of members of the Class, Plaintiff
16 understands that some 143 million U.S. consumers were affected by the breach, with over 15
17 million of those consumers being California residents. The number of affected consumers was
18 reported to the California Department of Justice, Office of the Attorney General by Equifax. The
19 class members thus appear readily ascertainable from records in Equifax’s possession, custody
20 and control. Indeed, Equifax has established a website specifically designed to allow consumers
21 to check if their data was compromised in the data breach.²⁸

22 40. Common questions of law and fact exist as to all members of each Class. This is
23 particularly true given the nature of the data breach, which affected all members of each Class,
24 thereby making appropriate relief with respect to each Class as a whole. Such common questions
25 of law and fact include but are not limited to:

- 26 a. Whether Equifax engaged in the unlawful conduct as herein alleged;

27
28 ²⁸ <https://www.equifaxsecurity2017.com/>

- 1 b. Whether Equifax owed a duty to the class members to protect their confidential
- 2 personal information;
- 3 c. Whether Equifax breached their duty to protect the confidential personal
- 4 information;
- 5 d. Whether Equifax knew or should have known of the vulnerabilities in its systems;
- 6 e. Whether Equifax was negligent in failing to address those vulnerabilities;
- 7 f. Whether Equifax knew or should have known about the vulnerabilities in its
- 8 systems before the data breach occurred;
- 9 g. Whether Equifax had a duty to notify class members of the data breach in a timely
- 10 manner;
- 11 h. Whether Equifax notified class members of the data breach in a timely manner;
- 12 i. The appropriate injunctive and related equitable relief for the Class; and
- 13 j. The appropriate class-wide measure of damages.

14 41. Plaintiff's claims are typical of the claims of the members of the Class, and
15 Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff and all members of
16 the Class are similarly affected by Equifax's conduct as their personal identifying information
17 was breached as a result of Equifax's conduct and they were harmed as a result of that conduct.

18 42. Plaintiff's claims arise out of the same common course of conduct giving rise to
19 the claims of the other members of the Class. Plaintiff's interests are coincident with, and not
20 antagonistic to, those of the other Class members. Plaintiff is represented by counsel, who are
21 competent and experienced in the prosecution of large-scale class action litigation.

22 43. The questions of law and fact common to the members of the Class are
23 predominant and outweigh those questions affecting only individual members, including legal
24 and factual issues relating to liability and damages.

25 44. Class action treatment is a superior method for the fair and efficient adjudication
26 of this litigation. With 143 million putative class members, class treatment will allow this
27 enormous number of similarly situated potential plaintiffs to prosecute their common claims in a
28

1 single forum in the most efficient manner. This will avoid the inevitable duplication of evidence,
2 effort, and expense that numerous individual actions would involve. The benefits of proceeding
3 through the class action mechanism, including providing injured persons or entities with a
4 method for obtaining redress for claims that might not be practicable to pursue individually and
5 significantly reducing the burden on the court system of trying these cases individually, far
6 outweigh any difficulties that may arise in the management of this class action.

7 **VI. CLAIMS FOR RELIEF**

8 **FIRST CAUSE OF ACTION: NEGLIGENCE**

9 **(Nationwide Negligence Class)**

10 45. Plaintiff incorporates and realleges, as though fully set forth herein, each and
11 every allegation set forth in the preceding paragraphs of this Complaint.

12 46. Equifax owed a duty to Plaintiff and the Class to protect the confidential personal
13 information stored on Equifax's systems. Equifax was well aware of the value of this
14 information and owed a duty to consumers to take all reasonable steps to ensure that the
15 information was protected and safeguarded from hacking attacks. Indeed, Equifax created the
16 risk of hacking: its business is dedicated to collecting and analyzing sensitive information about
17 consumers.

18 47. This duty to protect consumers' data is reflected in the law. California Civil Code,
19 Section 1798.81.5(b) requires that "A business that owns, licenses, or maintains personal
20 information about a California resident shall implement and maintain reasonable security
21 procedures and practices appropriate to the nature of the information, to protect the personal
22 information from unauthorized access, destruction, use, modification, or disclosure."

23 48. The risk of hacking was reasonably foreseeable. Equifax's own website warns of
24 the "sophisticated tactics" used by identity thieves to access personal information of the kind
25 accessed in this data breach.²⁹ Equifax had previous warning that hackers were targeting the
26 information in their possession and knew or should have known that they needed to take all

27 _____
28 ²⁹ <https://www.equifax.com/personal/education/identity-theft/how-to-protect-against-identity-theft>

1 reasonable steps to protect this information. The *New York Times* reported that last year, W-2 tax
2 and salary data was hacked from an Equifax website, while earlier this year, W-2 tax data was
3 hacked from TALX, an Equifax subsidiary.³⁰

4 49. Equifax knew or should have known that the vulnerability used by the hackers in
5 the data breach existed in their website applications. The information concerning the particular
6 website application vulnerability exploited in this data breach was freely available online as soon
7 as the vulnerability was discovered, along with reports that hackers were targeting this
8 vulnerability to access sensitive information. Equifax failed to secure its website applications
9 against these attacks, even though information concerning the vulnerability and how to patch it
10 was available two months before the data breach happened. As stated on Equifax's website, this
11 patch was not done until the days following Equifax's discovery of the data breach in late July.
12 Equifax failed to take the necessary steps to protect consumer data.

13 50. Plaintiff and the Class members' confidential personal information would not
14 have been compromised in this way if not for Equifax's failure to fulfill the duty it owed to
15 consumers to take reasonable steps to protect their data from hacking.

16 51. Neither Plaintiff nor the other Class Members contributed to the data breach or
17 Equifax's use of insufficient and below-industry standard security measures to safeguard
18 confidential personal information.

19 52. It was foreseeable that Equifax's failure to exercise reasonable care in protecting
20 the confidential personal information of consumers would result in Plaintiff and the other Class
21 Members suffering harm related to the loss of their personal information.

22 53. In advertising their products to consumers, Equifax states unequivocally on their
23 website: "being a victim of identity theft can be financially and emotionally devastating."³¹
24 Plaintiff and members of the Class have been harmed by having their personal information
25 accessed by unauthorized third parties. The full extent of the harm is unknown at this time but, at
26

27 ³⁰ <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html>

28 ³¹ <https://www.equifax.com/personal/education/identity-theft/how-to-protect-against-identity-theft>

1 the very least, Plaintiff and members of the Class have been forced to incur expenses to protect
2 themselves from identity theft, for example signing up for credit monitoring or fraud prevention
3 services, and will face further expenses to address any identity theft that occurs as a result of
4 Equifax's failure to keep consumer's personal information secure. As noted by Adam Levin,
5 chairman of CyberScout, in a quote to the New York Times: "The collateral damage can be
6 devastating, and when you are talking about Social Security numbers the only expiration date a
7 Social Security number has is yours."³²

8 54. Furthermore, Plaintiff and members of the Class face the ongoing risk of identity
9 theft as a result of this data breach. In addition to the expenses incurred to protect themselves, as
10 far as possible, from the use of their compromised data, Plaintiff and members of the Class now
11 face the inconvenience of stepping up their own monitoring of their credit report and related
12 activity to guard against signs of identity theft and the ongoing heightened risk of identity theft.

13 55. As a direct and proximate result of Equifax's negligent conduct, Plaintiff and the
14 Class have suffered injury and are entitled to damages in an amount to be proven at trial. Plaintiff
15 and the Class pray for relief as set forth below.

16 **SECOND CAUSE OF ACTION: Violation of California Customer Records Act**

17 **(Cal. Civil Code §§ 1798.80, et. seq.)**

18 **(California Class)**

19 56. Plaintiff incorporates and realleges, as through fully set forth herein, each and
20 every allegation set forth in the preceding paragraphs of this Complaint.

21 57. Pursuant to California Civil Code, Section 1798.81.5(b), "A business that owns,
22 licenses, or maintains personal information about a California resident shall implement and
23 maintain reasonable security procedures and practices appropriate to the nature of the
24 information, to protect the information from unauthorized access, destruction, use, modification,
25 or disclosure."

26 58. As described in detail above, Equifax failed to implement and maintain
27

28 ³² <https://www.nytimes.com/2017/09/08/business/equifax.html>

1 reasonable security procedures and practices to protect the confidential personal information it
2 maintained. Equifax’s failure to fix a vulnerability that it knew or should have known existed in
3 its website applications meant that unauthorized third parties were able to access, use, and/or
4 disclose consumers’ data.

5 59. Furthermore, pursuant to California Civil Code, Section 1798.82(a), any agency
6 that owns or licenses “computerized data that includes personal information” is required to
7 disclose any breach of the security of their systems to any California resident (1) whose
8 unencrypted personal information was acquired by an unauthorized person or (2) where both
9 encrypted personal information and the encryption key or security credential were both acquired.
10 This disclosure must be made “in the most expedient time possible and without unreasonable
11 delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to
12 determine the scope of the breach and restore the reasonable integrity of the data system.”

13 60. California Civil Code, Section 1798.82 (b) requires similar disclosures to the
14 owner or licensee of the information where an agency maintains but does not own the personal
15 information “immediately following discovery.”

16 61. Equifax knew of the breach for approximately 40 days before it notified
17 California consumers.

18 62. Plaintiff and the California Class were injured by these actions in that their
19 personal information was accessed, used, and/or disclosed by unauthorized third parties. Plaintiff
20 and the California Class have and will incur expenses to secure their private information and
21 address any identity theft that occurs as a result of Equifax’s failure to keep the personal
22 information of California residents secure. In addition to the expenses incurred to protect
23 themselves, as far as possible, from the use of their compromised data, Plaintiff and members of
24 the Class now face the inconvenience of stepping up their own monitoring of their credit report
25 and related activity to guard against signs of identity theft and the ongoing heightened risk of
26 identity theft.

27 63. Plaintiff and the California Class seek monetary damages pursuant to California
28

1 Civil Code, Section 1798.84(b). Plaintiff and the California Class also seek injunctive relief
2 pursuant to California Civil Code, Section 1798.84(e) to prevent any further violation of the
3 California Customer Records Act as a result of Equifax's lax security. Plaintiff and the Class
4 pray for relief as set forth below.

5 **THIRD CAUSE OF ACTION: Violation of Unfair Competition Law**

6 **(Cal. Bus. & Prof. Code §§ 17200 et seq.)**

7 **(California Class)**

8 64. Plaintiff incorporates and realleges, as though fully set forth herein, each and
9 every allegation set forth in the preceding paragraphs of this Complaint.

10 65. Equifax's unlawful, unfair and/or fraudulent business acts and practices –
11 particularly, their lax security in violation of the California Customer Records Act and
12 negligence in safeguarding the private personal information of some 15 million California
13 residents - harmed California consumers

14 66. Equifax's lax security measures are an unlawful violation of the California
15 Customer Records Act and directly resulted in the harm suffered by Plaintiff and the California
16 Class.

17 67. Equifax's delay in announcing the data breach is an unfair business practice that
18 left California consumers at heightened risk of identity theft for over a month. While Equifax
19 knew from July 29, 2017 that confidential personal information was accessed in the data breach,
20 this information was not disclosed to California consumers until September 7, 2017. This unfair
21 and improper delay in notifying California consumers of the breach left California consumers at
22 risk of identity theft. The inexcusable nature of this delay is compounded by reports that senior
23 Equifax executives sold off \$1.8 million of stock after the breach happened but before news of
24 the breach was made public.

25 68. Plaintiff and the California Class have and will suffer economic injury as a result
26 of Equifax's unlawful, unfair and/or fraudulent business practices. Plaintiff and the California
27 Class have and will incur expenses to secure their private information and address any identity
28

1 theft that occurs as a result of Equifax's failure to keep the confidential personal information of
2 California residents secure. Plaintiff and the California Class now also face the inconvenience of
3 vigilantly monitoring their credit report and use of their personal information for signs of identity
4 theft and the ongoing heightened risk of identity theft.

5 69. The harm suffered by Plaintiff and the California Class is directly linked to
6 Equifax's business acts and practices. Plaintiff and the California Class members' information
7 would not have been compromised in this way if not for Equifax's failure to fulfill the duty it
8 owed to consumers to take reasonable steps to protect their data from hacking.

9 70. Plaintiff and the California Class seek equitable relief directing full restitution of
10 all revenues, earnings, profits, compensation and benefits which may have been obtained by
11 Equifax as a result of its unlawful and unfair business acts and practices. Plaintiffs also seek
12 injunctive relief enjoining Equifax from engaging in the unlawful and unfair business practices
13 described herein in the future to ensure that Equifax takes all reasonable and necessary steps to
14 protect the confidential personal information it gathers from future hacking attempts.

15 **FOURTH CAUSE OF ACTION: Unjust Enrichment**

16 **(Nationwide Class)**

17 71. Plaintiff incorporates and realleges, as though fully set forth herein, each and
18 every allegation set forth in the preceding paragraphs of this Complaint.

19 72. Equifax knowingly received and retained benefits and funds from Plaintiff and
20 class members by compiling and using their confidential personal information and from the
21 amounts paid by any class members who purchased services from Equifax.

22 73. In addition, Equifax saved on the cost of providing adequate data security to
23 Plaintiff and the Class members. Equifax's cost savings came at the direct expense of the
24 security of Plaintiff and the Class members' confidential personal information.

25 74. Equifax appreciates and/or has knowledge of the benefits conferred upon it by
26 Plaintiff and the other class members.

1 75. As a result of Equifax's wrongful conduct, as described in detail herein, Equifax
2 has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the other Class
3 members.

4 76. Equifax's unjust enrichment is traceable to and directly and proximately results
5 from the wrongful conduct, as described in detail herein, including compiling and using Plaintiff
6 and the other Class members' confidential personal information without employing reasonable
7 security measures to keep that information safe from hackers.

8 77. It is inequitable to allow Equifax to retain the benefits they have received, and
9 continue to receive from Plaintiff and the other Class members. Plaintiff and the Class members
10 did not confer these benefits officiously or gratuitously and it would be inequitable and unjust for
11 Equifax to retain these profits.

12 78. Plaintiff and the Class members seek restitution in the amount of Equifax's
13 wrongfully obtained profits.

14 **V. PRAYER FOR RELIEF**

15 WHEREFORE, Plaintiffs respectfully request that the Court:

- 16 A. Determine that this action may be maintained as a class action under Rule 23(a),
17 (b)(2), and (b)(3) of the Federal Rules of Civil Procedure;
- 18 B. Direct that notice of this action, as provided by Rule 23(c)(2) of the Federal Rules
19 of Civil Procedure, be given to the Class;
- 20 C. Appoint Plaintiff as Class Representative and his counsel of record as Class
21 Counsel;
- 22 D. Enter judgment against Equifax and in favor of Plaintiff and the Class;
- 23 E. Adjudge and decree that the acts alleged herein by Plaintiff and the Class against
24 Equifax constitute negligence, violation of the California Customer Records Act,
25 violation of California's Unfair Competition Law, and unjust enrichment;
- 26 F. Award Plaintiff and the Class damages to the maximum extent allowed, including
27 actual and statutory damages;
- 28

1 G. Award restitution, including Equifax's wrongfully obtained profits, payable to
2 Plaintiff and the Class;

3 H. Award punitive damages, including treble and/or exemplary damages, to the
4 maximum extent allowed;

5 I. Award Plaintiff and the Class equitable, injunctive and declaratory relief as
6 appropriate under applicable laws, including an injunction permanently barring
7 continuation of the conduct complained of herein, and mandating that Defendant
8 and any successors in interest be required to adopt and implement appropriate
9 systems, controls, policies and procedures to protect the confidential personal
10 information of Plaintiff and the Class;

11 J. Award pre- and post-judgment interest at the highest legal rate;

12 K. Award Plaintiff and the Class members' reasonable attorneys' fees and costs of
13 suit; and

14 L. Award such other and further relief as the Court may deem just and proper.

15 ///

16 ///

17 ///

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28

1 **VI. DEMAND FOR JURY TRIAL**

2 Plaintiff hereby demands a jury trial on all claims so triable.

3
4 Dated: September 19, 2017

/s/ R. Alexander Saveri

5 R. Alexander Saveri (173102)
6 Geoffrey C. Rushing (126910)
7 Cadio Zirpoli (179108)
8 Sarah Van Culin (293181)
9 SAVERI & SAVERI, INC.
10 706 Sansome Street
11 San Francisco, CA 94111
12 Telephone: (415) 217-6810
13 Facsimile: (415) 217-6813
14 Email: rick@saveri.com;
15 geoff@saveri.com;
16 cadio@saveri.com; sarah@saveri.com

17
18
19
20
21
22
23
24
25
26
27
28
Randall Robinson Renick
HADSELL STORMER
RICHARDSON & RENICK, LLP
128 N. Fair Oaks Ave.
Pasadena, CA 91103
Telephone: (626) 585-9600
Facsimile: (626) 577-7079
Email: rrr@hadsellstormer.com

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Michael Branch

(b) County of Residence of First Listed Plaintiff Los Angeles, California (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number) R. Alexander Saveri, Saveri & Saveri, Inc., 706 Sansome Street San Francisco, CA 94111, (415) 217-6810

DEFENDANTS

Equifax, Inc.

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

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff 3 Federal Question (U.S. Government Not a Party) 2 U.S. Government Defendant 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship options: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding 2 Removed from State Court 3 Remanded from Appellate Court 4 Reinstated or Reopened 5 Transferred from Another District (specify) 6 Multidistrict Litigation-Transfer 8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. 1332 (d)

Brief description of cause:

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ According to Proof CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE Please see Attachment A DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) SAN FRANCISCO/OAKLAND SAN JOSE EUREKA-MCKINLEYVILLE

DATE 09/19/2017

SIGNATURE OF ATTORNEY OF RECORD

/s/ R. Alexander Saveri

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
- c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.

ATTACHMENT A – RELATED CASES

Judge	Docket Number
Hon. Beth Labson Freeman	5:17-cv-05228-BLF
Hon. Vince Chhabria	3:17-cv-05230-VC
Hon. Lucy H. Koh	5:17-cv-05265-LHK
Magistrate Judge Donna M. Ryu	3:17-cv-05284-DMR