

1 PHILLIP A. JARET, ESQ. [SBN 092212]  
2 ROBERT S. JARET, ESQ. [SBN 124876]  
3 JARET & JARET  
4 1016 Lincoln Avenue  
5 San Rafael, CA 94901  
6 Tel.: (415) 455-1010  
7 Fax: (415) 455-1050  
8 Email: *pajaret@jaretlaw.com*  
9 *rjaret@jaretlaw.com*

10 Attorneys for Plaintiff KAY EVANS,  
11 Individually and on Behalf of All Others  
12 Similarly Situated

13 U.S. DISTRICT COURT

14 NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

15	KAY EVANS, Individually and on Behalf of All Others Similarly Situated,	) Case No.
16	Plaintiffs,	) <b><u>CLASS ACTION COMPLAINT</u></b>
17	v.	) DEMAND FOR JURY TRIAL
18	EQUIFAX, INC.,	)
19	Defendant.	)

20 Plaintiff, Kay Evans, individually and on behalf of all those similarly situated, brings this  
21 action for damages and equitable relief against Equifax, Inc. and alleges on information and belief,  
22 as follows:

23 **I. NATURE OF CLAIMS**

24 1. This action arises as a result of Defendant Equifax, Inc.'s ("Equifax" or  
25 "Defendant") announcement on September 7, 2017 of the largest data breach in history. The  
26 hackers used a known vulnerability in an Equifax website application to gain access to confidential  
27 personal information including names, Social Security numbers, addresses, birth dates, and, in  
28 some instances, driver's license numbers of some 143 million people in the United States of  
America.

2. After discovering the hack on July 29, 2017, Equifax waited 40 days to disclose the  
data breach public, leaving consumers at high risk of identity theft for over one month.

1           3.       The hackers were able to gain access to this confidential personal information by  
2 exploiting a known Apache Struts vulnerability that had been publicized two months before the  
3 hack occurred. Equifax was negligent in failing to repair this known vulnerability and its failure  
4 to take reasonable security measures to protect consumer data means millions of Americans are  
5 now at risk of identity theft, which has caused them to incur expenses and inconvenience.

6           4.       Plaintiff and members of the proposed Classes have suffered harm and face the  
7 imminent risk of future harm. This includes the following:

- 8               a.       Costs associated with the detection and prevention of identity theft;
- 9               b.       Costs incurred in taking time to address the actual and future consequences  
10 of this data breach, including finding and challenging fraudulent changes to debit and credit  
11 accounts, cancelling credit cards, requesting purchase limits on compromised accounts, and the and  
12 annoyance of dealing with this data breach;
- 13              c.       Theft of their personal information;
- 14              d.       Impending threat of fraud and identity theft as a result of personal  
15 information being obtained by hackers and already misused and sold;
- 16              e.       Loss of use of and access to their accounts and costs associated with their  
17 inability to obtain money from their accounts or being limited in the amount of money they can  
18 obtain from their accounts, including missing payments, late charges and fees, and adverse effects  
19 on credit including decreased credit scores;
- 20              f.       Damage to the value of confidential personal information entrusted to  
21 Equifax for the sole purpose of reporting and/or monitoring their credit profile with the  
22 understanding that Equifax would safeguard Plaintiff and the Class members' data against theft;
- 23              g.       Monies paid for products purchased from Equifax (credit monitoring or  
24 credit score inquiries) at any time after July 29, 2017 when the data breach was discovered by  
25 Equifax; and
- 26              h.       Continued risk to their confidential personal information that is still in  
27 Equifax's possession and at risk of further breaches.

28 ///



1 Office of the Attorney General for the State of California that approximately 15,178,887 California  
2 residents were potentially impacted by the data breach.

3 11. Venue is proper in this District because Equifax is licensed to do business in and  
4 is doing business in this District, the Court has personal jurisdiction over Equifax, and because a  
5 substantial part of the events giving rise to the claim occurred in this District.

6 12. This action is not subject to arbitration. Equifax's website states:

7 [E]nrolling in the free credit file monitoring and identity theft  
8 protection that we are offering as part of this cybersecurity incident  
9 does not waive any rights to take legal action. We removed that  
10 language from the Terms of Use on the website,  
11 www.equifaxsecurity2017.com. The Terms of Use on  
12 www.equifax.com do not apply to the TrustedID Premier product  
13 being offered to consumers as a result of the cybersecurity  
14 incident.<sup>1</sup>

12 **IV. FACTUAL ALLEGATIONS**

13 13. There are three major credit reporting agencies in the United States—Equifax,  
14 Experian, and TransUnion.<sup>2</sup> These agencies are responsible for running the reports that are used to  
15 calculate consumers' credit scores; impacting their ability to get a mortgage, buy a car, or engage  
16 in any number of other financial transactions.<sup>3</sup>

17 14. Private information is at the core of Equifax's business. Equifax organizes and  
18 analyzes data on more than 820 million consumers and more than 91 million businesses worldwide.  
19 Its database includes employee data contributed from more than 7,100 employers.<sup>4</sup> Equifax operates

20 ///

22 ///

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

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

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

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

1 or has investments in 24 countries spanning North America, Central and South America, Europe  
2 and the Asia Pacific region.<sup>5</sup> Last year, Equifax made \$3.1 billion in revenue.<sup>6</sup>

3 15. Equifax is well aware of the private, sensitive nature of the information it stores.  
4 The Equifax website describes identity theft as "when someone steals your personal information  
5 – such as your name, Social Security number, and date of birth – typically to hijack your credit and  
6 use it to open up new credit accounts, take out loans in your name, or access your bank or  
7 retirement accounts."<sup>7</sup> The Equifax website also describes how this stolen information is used:

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

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

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

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

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

21 Set up a phone, wireless, or other utility service in your name.<sup>8</sup>

22 16. After describing these risks to consumers, Equifax suggests consumers to "Consider  
23 these Products" including "Equifax ID Patrol™," "Equifax ID Patrol™ Premier" and "Equifax  
24 Complete™ Advantage Plan" that claim to help consumers monitor their credit and protect their  
25 identity.

26 ///

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

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

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

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

1 17. The Equifax data breach is one of the largest breaches ever.<sup>9</sup> From mid-May  
2 through July 2017, "Criminals exploited a U.S. website application vulnerability to gain access to  
3 certain files" held by Equifax.<sup>10</sup> These files contained the names, Social Security numbers, birth  
4 dates, and addresses and, in some instances, driver's license numbers of some 143 million U.S.  
5 consumers.<sup>11</sup> In addition, the credit card numbers for approximately 209,000 U.S. consumers, and  
6 certain dispute documents with the personal identifying information for approximately 182,000  
7 U.S. consumers were accessed.<sup>12</sup> Equifax also identified unauthorized access to limited personal  
8 information for certain UK and Canadian residents.<sup>13</sup>

9 18. Approximately 15,178,887 California residents were potentially affected by this  
10 data breach.<sup>14</sup>

11 19. Equifax has stated that this breach was due to an Apache Struts vulnerability: "The  
12 vulnerability was Apache Struts CVE-2017-5638."<sup>15</sup>

13 20. The vulnerability identified by Equifax as the cause of this data breach had been  
14 discovered and patched some two months before the data breach.<sup>16</sup> Equifax did not update its  
15 website applications to fix this issue, despite reports back in March of 2017 that hackers were  
16 ///

---

19 <sup>9</sup> [http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-](http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX)  
20 [idUSKCN1BP1VX](http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX)

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

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

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

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

25 <sup>14</sup> [https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax -](https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach)  
26 [data breach; https://oag.ca.gov/system/files/Equifax%20-%20CA%20Letter\\_0.pdf](https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach)

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

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

1 actively targeting this vulnerability.<sup>17</sup> Instead Equifax's website indicates that patching of this  
2 vulnerability did not occur until late July 2017, after the breach had occurred:

3 On July 29, 2017, Equifax's Security team observed suspicious  
4 network traffic associated with its U.S. online dispute portal web  
5 application. In response, the Security team investigated and  
6 blocked the suspicious traffic that was identified.

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

11 The company's internal review of the incident continued. Upon  
12 discovering a vulnerability in the Apache Struts web application  
13 framework as the initial attack vector, Equifax patched the affected  
14 web application before bringing it back online.<sup>18</sup>

15 21. "Apache Struts is free, open-source software used to create Java web  
16 applications."<sup>19</sup> However, as noted by Boris Chen, vice president of engineering at tCell, in an  
17 interview with USA Today: "A single vulnerability in a web component should not result in  
18 millions of highly sensitive records being exfiltrated. Security controls should have existed at many  
19 points along the way to stop such a catastrophic outcome."<sup>20</sup>

20 22. Equifax discovered the data breach on July 29, 2017 but did not make this  
21 information public until September 7, 2017, some 40 days later, when Equifax issued a press  
22 release.<sup>21</sup>

23 23. While the public was misinformed about this massive breach, Equifax executives  
24 apparently were not. Three senior executives "sold \$1.8 million worth of shares in the days after  
25

---

26 <sup>17</sup> <https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imp-erils-high-impact-sites/>

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

28 <sup>19</sup> <https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/>

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

<sup>21</sup> <https://investor.equifax.com/news-and-events/news>

1 Equifax discovered the breach."<sup>22</sup> Equifax shares have dropped 32 percent since the company  
2 disclosed the breach.<sup>23</sup>

3 24. Equifax knew or should have known that its systems were at-risk of hacking attacks  
4 based on previous attacks and reports that its internal system had weaknesses. Equifax failed to  
5 improve its data security after two data breaches that occurred in the last year: one in which hackers  
6 took valuable W-2 tax and salary data, and, in another, hackers took W-2 tax data from an Equifax  
7 subsidiary called TALX.

8 25. The first Equifax security breach, which led to a class action lawsuit, stemmed from  
9 a May 2016 incident in which Equifax's W-2 Express website was breached, leading to the leak of  
10 430,000 names, addresses, social security numbers, and other information. Equifax had clients'  
11 employees access their data with default PIN numbers made up of the last four digits of their social  
12 security number and four digit year of birth; and assigned PIN numbers that were exceedingly easy  
13 for criminals to find on the internet. Equifax agreed to fix the underlying issue that led to this data  
14 breach, although it is unclear if the vulnerability has yet to be adequately addressed.

15 26. The second prior Equifax data breach involving TALX occurred because Equifax  
16 failed to discover that breach for almost a year—from April 17, 2016 through March 29, 2017. This  
17 breach was not publicly disclosed until May 2017. That security breach related to hackers using  
18 personal information to guess client customer questions and ultimately reset their 4-digit PIN to  
19 gain access to customers' tax data.

20 27. Equifax also suffered smaller data breaches in January 2017 concerning LifeLock  
21 customer credit information, and a 2013-2014 breach of credit reports using personal information.  
22 In 2016, a vulnerability to cross-site scripting was discovered. Cross-site scripting, also known as  
23 XSS, is a process by which an attacker could send a link they create to users who would click on  
24 the link and log on to the website, revealing their user names and passwords and jeopardizing their  
25 personal information.

---

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

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



1 28. There are several governmental investigations already underway. The FTC has  
2 confirmed that it is investigating the Equifax data breach.<sup>24</sup> The Consumer Financial Protection  
3 Bureau is also investigating Equifax. The Chairmen of the House Committee on Science, Space,  
4 and Technology and the House Committee on Oversight and Government Reform have said that  
5 their respective committees will investigate the Equifax data breach and have requested that  
6 Equifax produce documents by September 28, 2017.<sup>25</sup> Equifax CEO Richard Smith is scheduled  
7 to appear at a hearing on the House Subcommittee on Digital Commerce and Consumer Protection  
8 on October 3, 2017.<sup>26</sup> The Federal Bureau of Investigation has opened an investigation into the  
9 breach, along with nearly 40 states.<sup>27</sup>

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

13 30. Even if consumers freeze their credit reports with Equifax, they must also freeze  
14 them for Experian and TransUnion as well to give them the best protection.

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

17 32. Furthermore, even if consumers freeze their credit reports, they are not protected  
18 from fraudulent tax returns being filed with their information or people using their credit cards.

19 ///

20 ///

---

22 <sup>24</sup> [http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-](http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX)  
23 <https://www.usatoday.com/story/money/2017/09/14/ftc-investigating-equifax-over-data-breach/665550001/>

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

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

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

V. CLASS ALLEGATIONS

33. Plaintiff brings this class action pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(2) and (b)(3) on her own behalf and as representative of the following classes of persons and entities (the "Classes").

34. A nationwide "Negligence Class" seeking damages, equitable and injunctive relief:

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

And a "California Class" seeking damages, equitable and injunctive relief:

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

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

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

---

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

1           a.       Whether Equifax engaged in unlawful conduct and unfair business  
2 practices, as herein alleged;

3           b.       Whether Equifax owed a duty to the class members to protect their  
4 confidential personal information;

5           c.       Whether Equifax breached their duty to protect the confidential personal  
6 information;

7           d.       Whether Equifax knew or should have known that its computer systems  
8 were vulnerable to hacking;

9           e.       Whether Equifax was negligent in failing to address those vulnerabilities;

10          f.       Whether Equifax knew or should have known about the vulnerabilities in  
11 its systems before the data breach occurred;

12          g.       Whether Equifax had a duty to notify class members of the data breach in  
13 a timely manner;

14          h.       Whether Equifax notified class members of the data breach in a timely  
15 manner;

16          i.       Whether Equifax's conduct constitutes an unfair business practice under  
17 the UCL (Unfair Competition Law) for violating the Gramm-Leach-Bliley Act (GLBA).

18          j.       Whether Equifax acted willfully and/or with oppression, fraud, or malice;

19          k.       The appropriate injunctive and related equitable relief for the Class; and

20          l.       The appropriate class-wide measure of damages.

21          37.       Plaintiff's claims are typical of the claims of the members of the Class, and Plaintiff  
22 will fairly and adequately protect the interests of the Class. Plaintiff and all members of the Class  
23 are similarly affected by Equifax's conduct as their personal identifying information was breached  
24 as a result of Equifax's conduct and they were harmed as a result of that conduct.

25          38.       Plaintiff's claims arise out of the same common course of conduct giving rise to the  
26 claims of the other members of the Class. Plaintiff's interests are coincident with, and not  
27 antagonistic to, those of the other Class members. Plaintiff is represented by counsel, who are  
28 competent and experienced in the prosecution of action litigation.

1           39.        The questions of law and fact common to the members of the Class are predominant  
2     and outweigh those questions affecting only individual members, including legal and factual issues  
3     relating to liability and damages.

4           40.        Class action treatment is a superior method for the fair and efficient adjudication  
5     of this litigation. With 143 million putative class members, class treatment will allow this enormous  
6     number of similarly situated potential plaintiffs to prosecute their common claims in a single forum  
7     in the most efficient manner. This will avoid the inevitable duplication of evidence, effort, and  
8     expense that numerous individual actions would involve. The benefits of proceeding through the  
9     class action mechanism, including providing injured persons or entities with a method for obtaining  
10    redress for claims that might not be practicable to pursue individually and significantly reducing  
11    the burden on the court system of trying these cases individually, far outweigh any difficulties that  
12    may arise in the management of this class action.

13   **VI. CLAIMS FOR RELIEF**

14   **FIRST CAUSE OF ACTION**

15   **Negligence**

16   **(Nationwide Class)**

17           41.        Plaintiff incorporates and realleges, as though fully set forth herein, each and every  
18    allegation set forth in this Complaint.

19           42.        Equifax owed a duty to Plaintiff and the Class to protect the confidential personal  
20    information stored on Equifax's systems. Equifax was well aware of the value of this information  
21    and owed a duty to consumers to take all reasonable steps to ensure that the information was  
22    protected and safeguarded from hacking. Equifax created the risk of hacking. Its business is  
23    dedicated to collecting and analyzing sensitive information about consumers.

24           43.        This duty to protect consumers' data is codified. California Civil Code, Section  
25    1798.81.5(b) requires that "A business that owns, licenses, or maintains personal information about  
26    a California resident shall implement and maintain reasonable security procedures and practices  
27    appropriate to the nature of the information, to protect the personal information from unauthorized  
28    access, destruction, use, modification, or disclosure."

1           44.       The risk of hacking was reasonably foreseeable. Equifax's own website warns of  
2 the "sophisticated tactics" used by identity thieves to access personal information of the kind  
3 accessed in this data breach.<sup>29</sup> Equifax had previous warning that hackers were targeting the  
4 information in their possession and knew or should have known that they needed to take all  
5 reasonable steps to protect this information. The New York Times reported that last year, W-2 tax  
6 and salary data was hacked from an Equifax website, while earlier this year, W-2 tax data was  
7 hacked from TALX, an Equifax subsidiary.<sup>30</sup>

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

17           46.       Plaintiff and the Class members' confidential personal information would not have  
18 been compromised in this way but for Equifax's failure to fulfill the duty it owed to consumers to  
19 take reasonable steps to protect their data from hacking.

20           47.       Neither Plaintiff nor the other Class Members contributed to the data breach or  
21 Equifax's use of insufficient and below-industry standard security measures to safeguard  
22 confidential personal information.

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

---

26  
27           <sup>29</sup> <https://www.equifaxsecurity2017.com/>

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

1           49. In advertising their products to consumers, Equifax states unequivocally on its  
2 website: "being a victim of identity theft can be financially and emotionally devastating."<sup>31</sup> Plaintiff  
3 and members of the Class have been harmed by having their personal information accessed by  
4 unauthorized third parties. The full extent of the harm is unknown at this time but Plaintiff and  
5 members of the Class have been forced to incur expenses to protect themselves from identity theft,  
6 for example signing up for credit monitoring or fraud prevention services, and will face further  
7 expenses to address any identity theft that occurs as a result of Equifax's failure to keep consumer's  
8 personal information secure. As noted by Adam Levin, chairman of CyberScout, in a quote to the  
9 New York Times: "The collateral damage can be devastating, and when you are talking about  
10 Social Security numbers the only expiration date a Social Security number has is yours."<sup>32</sup>

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

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

19   **SECOND CAUSE OF ACTION**

20                           **Violation of Credit Repair Organizations Act, 15 U.S.C. §§ 1679a et seq.**

21   **(Nationwide Class)**

22           52. Plaintiff incorporates and realleges, as though fully set forth herein, each and every  
23 allegation set forth in this Complaint.

24           53. Equifax is a "person" within the meaning of 15 U.S. Code § 1679b. Equifax is also  
25 a credit repair organization within the meaning of 15 U.S.C. § 1679a(3), because, among other

26 \_\_\_\_\_  
27           <sup>31</sup> <https://www.equifax.com/personal/education/identity-theft/how-to-protect-against-identity-theft>

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

1 things, it uses an instrumentality of interstate commerce or the mail to sell, provide, or perform (or  
2 represent that it will sell, provide, or perform) services in exchange for money or other valuable  
3 consideration for the express or implied purposes of advising and assisting consumers concerning  
4 their credit history, activity, record, and credit rating.

5 54. TrustedID is a credit repair organization within the meaning of 15 U.S.C. §  
6 1679a(3), because, among other things, it uses an instrumentality of interstate commerce or the mail  
7 to sell, provide, or perform (or represent that it will sell, provide, or perform) services in exchange  
8 for money or other valuable consideration for the express or implied purposes of advising and  
9 assisting consumers concerning their credit history, activity, record, and credit rating.

10 55. The Credit Repair Organizations Act makes it unlawful to engage, directly or  
11 indirectly, in any act, practice, or course of business that constitutes or results in the commission  
12 of, or an attempt to commit, a fraud or deception on any person in connection with the offer or sale  
13 of the services of the credit repair organization, or to make or use any untrue or misleading  
14 representation of the services of a credit repair organization.

15 56. During the time that Equifax had knowledge of the Data Breach, but was  
16 withholding that knowledge from consumers, it engaged in misleading representations in  
17 connection with offering services for the purposes of advising and assisting consumers concerning  
18 their credit history, activity, record, and credit rating, including without limitation:

19 a. advertising and selling services that purported to allow consumers to  
20 “control” their financial lives;

21 b. advertising and selling services that purported to help consumers fix  
22 inaccurate credit information and “restore” their credit information;

23 c. advertising and selling services that purported to help consumers get out  
24 of debt;

25 d. advertising and selling services that purported to inform and alert  
26 consumers to unusual activity in connection with their personal and financial information;

27 e. advertising and selling services that purportedly allowed consumers to  
28 decide by whom and when their Equifax credit files would be seen; and

1 f. representing to governmental, corporate, and other entities providing  
2 information to Equifax, including consumers, that Equifax's cyber security was adequate to protect  
3 such information.

4 57. During the time that Equifax had knowledge of the Data Breach, but was  
5 withholding that knowledge from consumers, Equifax intentionally failed to disclose material facts,  
6 which it had a duty to disclose to them, concerning the existence, nature, and circumstances of the  
7 Data Breach.

8 58. During the time that Equifax had knowledge of the Data Breach, but was  
9 withholding that knowledge from consumers, Plaintiff Kay Evans and other members of the Class  
10 paid Equifax or its affiliated or wholly-owned companies for services concerning their credit  
11 history, activity, record, and credit rating.

12 59. Equifax engaged in material misrepresentations or omissions of its services to  
13 induce Americans and certain members of the Class to enroll in Equifax's TrustedID credit  
14 services, for the purposes of obtaining further sensitive PII from such enrollees, and with the  
15 expectation that many such persons would renew their enrollment in TrustedID beyond the one year  
16 free period, by:]

17 a. affirmatively misrepresenting to consumers and the public that the  
18 dedicated Equifax breach website would inform individuals whether their information had been  
19 compromised in the Data Breach, when in fact the website provided, and provides, no meaningful  
20 answers but instead collects and stores users' names and Social Security numbers and puts them  
21 on a waitlist to enroll with TrustedID;

22 b. omitting material information regarding TrustedID, including that it is a  
23 wholly-owned subsidiary of Equifax, and that registering for the service purported to waive an  
24 individual's right to pursue claims against Equifax or TrustedID in a court of law; and c.  
25 affirmatively misrepresenting whether minors could have been affected by the Data Breach,  
26 including by expressly excluding them from coverage under the one-year trial offered through  
27 TrustedID and by making false statements on the dedicated breach website to the effect that  
28 Equifax does not store information concerning minors.



1 60. The above conduct was directed toward hundreds of millions of consumers, was  
2 frequent in terms of the nature of such noncompliance, and was intentional and intended to position  
3 Equifax to profit from Americans' reaction to the Data Breach.

4 61. As a result of Equifax's conduct alleged herein, pursuant to the Credit Repair  
5 Organizations Act, Equifax is strictly liable to the Class for all monies paid to Equifax by members  
6 of the Class under these false pretenses.

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

10 **THIRD CAUSE OF ACTION**

11 **Violation of California Customer Records Act**

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

13 **(California Class)**

14 63. Plaintiff incorporates and realleges, as though fully set forth herein, each and every  
15 allegation set forth in this Complaint.

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

20 65. As described in detail above, Equifax failed to implement and maintain reasonable  
21 security procedures and practices to protect the confidential personal information it maintained.  
22 Equifax's failure to fix a vulnerability that it knew or should have known existed in its website  
23 applications meant that unauthorized third parties were able to access, use, and/or disclose  
24 consumers' data.

25 66. Furthermore, pursuant to California Civil Code, Section 1798.82(a), any agency that  
26 owns or licenses "computerized data that includes personal information" is required to disclose any  
27 breach of the security of their systems to any California resident (1) whose unencrypted personal  
28 information was acquired by an unauthorized person or (2) where both encrypted personal

1 information and the encryption key or security credential were both acquired. This disclosure must  
2 be made "in the most expedient time possible and without unreasonable delay, consistent with the  
3 legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the  
4 breach and restore the reasonable integrity of the data system."

5 67. California Civil Code, Section 1798.82 (b) requires similar disclosures to the owner  
6 or licensee of the information where an agency maintains but does not own the personal  
7 information "immediately following discovery."

8 68. Equifax knew of the breach for approximately 40 days before it notified California  
9 consumers.

10 69. Plaintiff and the California Class were injured by these actions in that their personal  
11 information was accessed, used, and/or disclosed by unauthorized third parties. Plaintiff and the  
12 California Class have and will incur expenses to secure their private information and address any  
13 identity theft that occurs as a result of Equifax's failure to keep the personal information of  
14 California residents secure. In addition to the expenses incurred to protect themselves, as far as  
15 possible, from the use of their compromised data, Plaintiff and members of the Class now face the  
16 inconvenience of stepping up their own monitoring of their credit report and related activity to  
17 guard against signs of identity theft and the ongoing heightened risk of identity theft.

18 70. Plaintiff and the California Class seek monetary damages pursuant to California  
19 Civil Code, Section 1798.84(b). Plaintiff and the California Class also seek injunctive relief  
20 pursuant to California Civil Code, Section 1798.84(e) to prevent any further violation of the  
21 California Customer Records Act as a result of Equifax's lax security. Plaintiff and the Class pray  
22 for relief as set forth below.

23 **FOURTH CAUSE OF ACTION**

24 **Violation of Unfair Competition Law**

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

26 **(California Class)**

27 71. Plaintiff incorporates and realleges, as though fully set forth herein, each and every  
28 allegation set forth in this Complaint.

1           72.       Equifax's unlawful, unfair and/or fraudulent business acts and practices,  
2 particularly, their lax security in violation of the California Customer Records Act and negligence  
3 in safeguarding the private personal information of some 15 million California residents, has  
4 harmed California consumers.

5           73.       Equifax's lax security measures are an unlawful violation of the California Customer  
6 Records Act and directly resulted in the harm suffered by Plaintiff and the California Class.

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

15           75.       Plaintiff and the California Class have and will suffer economic injury as a result  
16 of Equifax's unlawful, unfair and/or fraudulent business practices. Plaintiff and the California Class  
17 have and will incur expenses to secure their private information and address any identity theft that  
18 occurs as a result of Equifax's failure to keep the confidential personal information of California  
19 residents secure. Plaintiff and the California Class now also face the inconvenience of vigilantly  
20 monitoring their credit report and use of their personal information for signs of identity theft and  
21 the ongoing heightened risk of identity theft.

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

26           77.       Plaintiff and the California Class seek equitable relief directing full restitution of  
27 all revenues, earnings, profits, compensation and benefits which may have been obtained by  
28 Equifax as a result of its unlawful and unfair business acts and practices. Plaintiffs also seek

1 injunctive relief enjoining Equifax from engaging in the unlawful and unfair business practices  
2 described herein in the future to ensure that Equifax takes all reasonable and necessary steps to  
3 protect the confidential personal information it gathers from future hacking attempts.

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

7 **FIFTH CAUSE OF ACTION**

8 **Unjust Enrichment**

9 **(Nationwide Class)**

10 79. Plaintiff incorporates and realleges, as though fully set forth herein, each and every  
11 allegation set forth in this Complaint.

12 80. Equifax knowingly received and retained benefits and funds from Plaintiff and class  
13 members by compiling and using their confidential personal information and from the amounts paid  
14 by any class members who purchased services from Equifax.

15 81. In addition, Equifax saved on the cost of providing adequate data security to  
16 Plaintiff and the Class members. Equifax's cost savings came at the direct expense of the security  
17 of Plaintiff and the Class members' confidential personal information.

18 82. Equifax is aware of the benefits conferred upon it by Plaintiff and the other class  
19 members.

20 83. As a result of Equifax's wrongful conduct, as described in detail herein, Equifax has  
21 been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the other Class  
22 members.

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

27 85. It is inequitable to allow Equifax to retain the benefits they have received, and  
28 continue to receive from Plaintiff and the other Class members.

1 86. Plaintiff and the Class members seek restitution in the amount of Equifax's  
2 wrongfully obtained profits.

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

6 **V. PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiffs respectfully request that the Court:

8 A. Determine that this action may be maintained as a class action under Rule  
9 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure;

10 B. Direct that notice of this action, as provided by Rule 23(c)(2) of the  
11 Federal Rules of Civil Procedure, be given to the Class;

12 C. Appoint Plaintiff as Class Representative and her counsel of record as  
13 Class Counsel;

14 D. Enter judgment against Equifax and in favor of Plaintiff and the Class;

15 E. Adjudge and decree that the acts alleged herein by Plaintiff and the Class  
16 against Equifax constitute negligence, violation of the Credit Repair Organizations Act, violation  
17 of the California Customer Records Act, violation of California's Unfair Competition Law, and  
18 unjust enrichment;

19 F. Award Plaintiff and the Class damages to the maximum extent allowed,  
20 including actual and statutory damages;

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

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

25 I. Award Plaintiff and the Class equitable, injunctive and declaratory relief  
26 as appropriate under applicable laws, including an injunction permanently barring continuation of  
27 the conduct complained of herein, and mandating that Defendant and any successors in interest be  
28 required to adopt and implement appropriate systems, controls, policies and procedures to protect

1 the confidential personal information of Plaintiff and the Class;

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

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

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

6 **VI. DEMAND FOR JURY TRIAL**

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

8

9 DATED: September 20, 2017

10

By: /s/ PHILLIP A. JARET

11

JARET & JARET  
Phillip A. Jaret  
Robert S. Jaret  
1016 Lincoln Ave.  
San Rafael, CA 94901  
Tel.: (415) 455-1010  
Fax.: (415) 455-1050

12

13

14

15

Attorneys for Plaintiff KAY EVANS, Individually  
and on Behalf of All Others Similarly Situated

16

17

18

19

20

21

22

23

24

25

26

27

28

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

KAY EVANS, Individually and on Behalf of All Others Similarly Situated,

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

(c) Attorneys (Firm Name, Address, and Telephone Number) Jaret & Jaret, 1016 Lincoln Avenue, San Rafael, CA 94901, tel. (415) 455-1010

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):

Brief description of cause:

Negligence; Violation of Cal. Civil Code §§ 1798.80, et seq.; Unfair Competition Law and Unjust Enrichment

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$

CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

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

JUDGE

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 09/20/2017

SIGNATURE OF ATTORNEY OF RECORD

/s/ Phillip A. Jaret, Esq.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

KAY EVANS, Individually and on Behalf of All Others Similarly Situated

Plaintiff(s)

v.

EQUIFAX, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

Equifax, Inc.
1550 Peachtree Street N.W.
Atlanta, GA 30309-2402
C/O CSC - Lawyers Incorporating Service
2710 Gateway Oaks Dr., Suite 150N, Sacramento, CA 95833

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Phillip A. Jaret, Esq. [SBN 092212]
JARET & JARET
1016 Lincoln Avenue
San Rafael, CA 94901

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk



Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*: \_\_\_\_\_  
\_\_\_\_\_ .

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc: