

1 Helen I. Zeldes (SBN 220051)
David Peck (SBN 171854)
2 Lauren Stewart (SBN 309893)
3 **COAST LAW GROUP, LLP**
1140 S. Coast Hwy 101
4 Encinitas, CA 92024
5 Tel: (760) 942-8505
6 Fax: (760) 942 -8515
helen@coastlaw.com

7 Tammy Gruder Hussin (SBN 155290)
8 **HUSSIN LAW**
9 1596 N. Coast Highway 101
Encinitas, CA 92024
10 Tel: (877) 677-5397
11 Fax: (877) 667-1547
tammy@hussinlaw.com

12
13 Attorneys for Plaintiffs Christopher Tanks, Brittany Dixon
14 and the Putative Class

15
16 **UNITED STATES DISTRICT COURT**
17 **SOUTHERN DISTRICT OF CALIFORNIA**

18
19 CHRISTOPHER TANKS and
20 BRITTANY DIXON, on behalf of
21 themselves and all others similarly
situated,

22 Plaintiffs,

23 vs.

24
25 EQUIFAX, INC., a Georgia
26 corporation; and DOES 1-10,
inclusive,

27 Defendants.
28

Civil Case No.: '17CV1832 BAS BLM

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiffs Christopher Tanks and Brittany Dixon (“Plaintiffs”), individually and
2 on behalf of all others similarly situated, allege on personal knowledge, investigation of
3 their counsel, and on information and belief as follows:

4 **NATURE OF THE ACTION**

5 1. In today's world, where the nefarious acquisition, collection and
6 dissemination of personal data can literally sway national elections, and where
7 breaches of data collected by massive corporations can lead to misery for millions of
8 consumers, Equifax's cavalier attitude for the safety and security of private
9 information is truly breathtaking. Plaintiffs bring this action for damages, and other
10 legal and equitable remedies, resulting from the reckless and illegal actions of Equifax,
11 Inc. (“Equifax”) related to an unprecedented massive breach of database security (the
12 “Data Breach”). The Data Breach resulted in over 143 million individuals’ – nearly
13 half the population of the United States - Personally Identifiable Information (“PII”)
14 being stolen from Equifax’s databases.

15 2. Equifax’s failure to adequately protect consumers’ most sensitive
16 information has far reaching implications. The stolen PII includes detailed personal
17 data, including names, social security numbers, birth dates, addresses, driver’s license
18 numbers, credit card numbers, bank account numbers, and more.

19 3. According to Equifax’s September 7, 2017 press release, Equifax
20 acknowledged it experienced “a cybersecurity incident potentially impacting
21 approximately 143 million U.S. consumers. Criminals exploited a U.S. website
22 application vulnerability to gain access to certain files. Based on the company’s
23 investigation, the unauthorized access occurred from mid-May through July 2017.”

24 4. Equifax claims it discovered the breach on July 29, 2017, yet it did
25 nothing to notify affected consumers until September 8, 2017, leaving Plaintiffs and
26 half of America vulnerable to identity thieves. As of the date of the filing of this
27 complaint, Equifax still has not bothered to notify Plaintiffs or Class Members of the
28 Data Breach. Meanwhile, Equifax’s top executives have been busy protecting

1 themselves rather than focusing on Plaintiffs' vulnerabilities, selling off millions of
2 dollars of their stock before notifying the public. Other stock trading activity
3 suggests other insiders secretly traded Equifax stock, capitalizing on their knowledge
4 there would be a dramatic decline of the stock following the announcement.

5 5. The Data Breach was a direct result of Equifax's failure to implement
6 adequate security measures to safeguard consumers' PII. Equifax willfully ignored
7 known weaknesses in its data security, including prior hacks into its information
8 systems. Unauthorized parties routinely attempt to gain access to and steal personal
9 information from networks and information systems, like Equifax. Inasmuch as
10 Equifax is known to possess a massive amount of our nation's PII, Equifax had a duty
11 to implement effective procedures to avoid a breach of this magnitude. Equifax utterly
12 failed in its duty, causing potential harm of gargantuan proportions – potentially
13 impacting consumers for life.

14 6. Equifax's failure to adequately protect the PII of Plaintiffs and Class
15 Members will allow identity thieves to commit a variety of crimes that harm victims of
16 the Data Breach. For instance, the thieves can take out loans, mortgage property, open
17 bank accounts and credit cards in a victim's name; use a victim's information to obtain
18 government benefits or file fraudulent returns to obtain a tax refund, obtain a driver's
19 license or identification card in a victim's name, gain employment in a victim's name,
20 obtain medical services in a victim's name, and/or give false information to police
21 during an arrest. Hackers also routinely sell individuals' PII to other nefarious
22 individuals who intend to misuse the information.

23 7. As a direct result of Equifax's willful failure to prevent the Data Breach,
24 Plaintiffs and Class Members have been exposed to a significant likelihood of fraud,
25 identity theft, and financial harm, as detailed below, and to a substantial, heightened,
26 and imminent risk of such harm in the near and indefinite future.

27 8. There is a substantial likelihood that Class Members already have or will
28 become victims of identity fraud given the breadth of information about them that is

1 now in the hands of wrong doers. Javelin Strategy & Research reported in its 2014
2 Identity Fraud Study that “[d]ata breaches are the greatest risk factor for identity
3 fraud.” In fact, “[i]n 2013, *one in three* consumers who received notification of a data
4 breach became a victim of fraud.” Javelin also found increased instances of fraud other
5 than credit card fraud, including “compromised lines of credit, internet accounts (e.g.,
6 eBay, Amazon) and email payment accounts such as PayPal.” (emphasis added).

7 9. Plaintiffs and other members of the class never asked Equifax to store
8 their data. Now, as a result of Equifax’s failures, Plaintiffs and Class Members are
9 forced to monitor their financial accounts and credit histories more closely and take
10 extra precautions to guard against identity theft.

11 10. Plaintiffs and Class Members also have incurred, and will continue to
12 incur, additional out-of-pocket costs for obtaining credit reports, credit freezes, credit
13 monitoring services, and other protective measures in order to detect, protect, and
14 repair the Data Breach’s impact on their PII for the remainder of their lives. Going
15 forward, Plaintiffs and Class Members anticipate spending considerable time and
16 money in order to detect and respond to the impacts of the Data Breach.

17 11. In an effort to minimize the harm it caused, Equifax has offered a year of
18 credit protection using its own company, TrustedID. Yet the offer falls far short. The
19 identity thieves have obtained so much PII they are highly unlikely to cease fraudulent
20 activity after twelve months, and as a result Plaintiffs and Class Members will require
21 a lifetime of credit protection. Moreover, inasmuch as Equifax’s incompetence is the
22 cause of the Data Breach, Plaintiffs and Class Members have zero faith that Equifax’s
23 credit protection company would be an effective and reliable source of protection.

24 12. Plaintiffs bring this action to remedy these harms on behalf of themselves
25 and all similarly situated individuals whose PII was accessed during the Data Breach.
26 Plaintiffs seeks to recover damages, including actual and statutory damages, equitable
27 relief, reimbursement of out-of-pocket losses, other compensatory damages, a lifetime
28 of credit monitoring services with accompanying identity theft insurance, and

1 injunctive relief including an order requiring Equifax to implement improved data
2 security measures.

3 **JURISDICTION AND VENUE**

4 13. This matter in controversy exceeds \$5,000,000 and the class is comprised
5 of tens of millions of individuals. Accordingly, this Court has jurisdiction pursuant to
6 28 U.S.C. § 1332(d)(2). Further, Plaintiffs allege a national class, which will result in
7 at least one Class Member belonging to a different state. Therefore, both elements of
8 diversity jurisdiction under the Class Action Fairness Act of 2005 (“CAFA”) are
9 present, and this Court has jurisdiction. This Court also has federal question
10 jurisdiction pursuant to 28 U.S.C. § 1331.

11 14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)-(c) and
12 1441(a), in that Defendant is deemed to reside in any judicial district in which it is
13 subject to personal jurisdiction at the time the action is commenced; Defendant’s
14 contacts within this District are sufficient to subject it to personal jurisdiction; and a
15 substantial portion of the acts giving rise to this action occurred in this District.

16 **PARTIES**

17 15. Plaintiff, Christopher Tanks, is, and at all times mentioned herein was, an
18 individual citizen of the State of California and resides in San Diego County,
19 California.

20 16. Plaintiffs Brittany Dixon is, and at all times mentioned herein was, an
21 individual citizen of the State of California and resides in Los Angeles County,
22 California.

23 17. Defendant Equifax, Inc. is incorporated in Georgia with its headquarters
24 and principal place of business located at 1550 Peachtree Street, N.W., Atlanta,
25 Georgia 30309.

26 18. Equifax is one of the major credit reporting agencies in the United States.
27 As a credit bureau service, Equifax is engaged in a number of credit-related services,
28 as described by Equifax “[t]he company organizes, assimilates and analyzes data on

1 more than 800 million consumers and more than 88 million business worldwide, and
2 its database includes employee data contributed from more than 5,000 employers.”

3 **FACTUAL ALLEGATIONS**

4 **Equifax’s Unprecedented Data Breach**

5 19. Starting in mid-May of 2017 and continuing on for at least *ten weeks*,
6 identity thieves absconded with half of the United States’ citizens’ critically sensitive
7 PII while Equifax was asleep at the wheel. Equifax claims it learned of this tidal wave
8 of a breach on July 29, 2017. Instead of taking steps to notify consumers on a timely
9 basis, Equifax’s executives ran off with millions of dollars in profits selling their
10 shares in the days before they made their massive blunder known.

11 20. Equifax’s computer database and systems were accessed by unauthorized
12 users who stole the PII of approximately 143 million individuals, including names,
13 Social Security numbers, birth dates, addresses, driver’s license numbers, credit card
14 numbers, and certain “dispute documents.”

15 21. Equifax discovered the breach on July 29, 2017 but did nothing to
16 disclose the massive breach to the public until September 8, 2017. As of the date of
17 the filing of this complaint, Equifax had still not notified Plaintiffs of the Data
18 Breach.

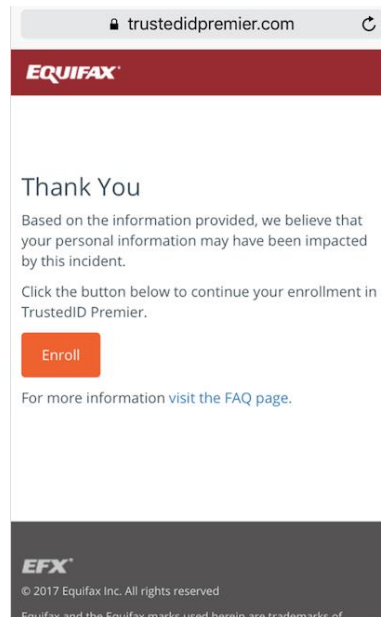
19 22. Plaintiffs and Class Members have suffered harm as a result of Equifax’s
20 negligence and willful ignorance in the form of additional out-of-pocket costs for
21 obtaining credit reports, credit freezes, credit monitoring services, and other protective
22 measures in order to detect, protect, and repair the Data Breach’s impact on their PII
23 for the remainder of their lives. Going forward, Plaintiffs and Class Members
24 anticipate spending considerable time and money in order to detect and respond to the
25 impact of the Data Breach.

26 23. Prior to the Data Breach, Equifax promised to safeguard its consumers’
27 PII: “We have built our reputation on our commitment to deliver reliable
28 information to our customers (both businesses and consumers) and to protect the

1 privacy and confidentiality of personal information about consumers. We also protect
2 the sensitive information we have about businesses. Safeguarding the privacy and
3 security of information, both online and offline, is a top priority for Equifax.”¹
4 Equifax failed consumers dramatically.

5 **Plaintiffs’ PII Was Fraudulently Used During the Data Breach**

6 24. **Christopher Tanks:** Mr. Tanks learned about the Equifax data breach
7 like the rest of the world on September 7, 2017. On September 9, 2017, Mr. Tanks
8 used Equifax’s online lookup tool to check and see if his PII was impacted by the
9 Equifax data breach received this message:

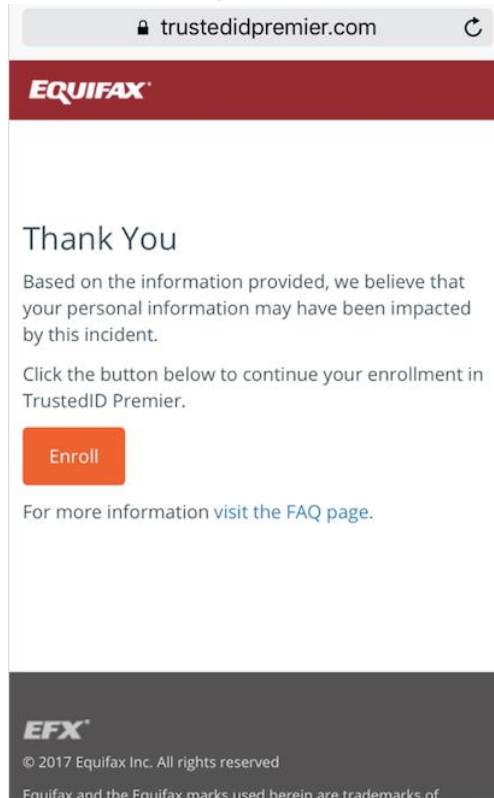


10
11
12
13
14
15
16
17
18
19
20 25. On or about the last week of July of 2017 – during the time frame
21 Equifax disclosed its massive data breach occurred -- Mr. Tanks learned that his
22 identity had been stolen and someone had run an unauthorized \$25.00 charge through
23 his bank account. Mr. Tanks filed a fraud claim with his bank and was issued a new
24 debit card.

25 26. **Brittany Dixon:** Ms. Dixon learned about the Equifax data breach like
26 the rest of the world on September 7, 2017. On September 9, 2017, Ms. Dixon used
27 Equifax’s online lookup tool to check and see if her PII was impacted by the Equifax
28

¹ <http://www.equifax.com/privacy/>

1 data breach and received this message:



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

27. During May and June of 2017 – during the time frame Equifax claims its massive data breach occurred – an identity thief attempted to use Ms. Dixon’s PII to open accounts in her name. Ms. Dixon was successful in removing the fraudulent accounts from her credit report, but worries of further attempts to use her identity.

28. Upon learning from Equifax that their PII may have been impacted by Equifax’s data breach, and while knowing fraudulent activity occurred during the relevant timeframe, Plaintiffs subscribed to a credit monitoring program. Although Equifax offered Plaintiffs free credit protection for a year, Plaintiffs will require a lifetime of credit protection.

29. Moreover, Plaintiffs have no interest in enrolling in a credit protection service with the very company that grossly mishandled their PII in the first place. Plaintiffs and Class Members do not have faith that Equifax’s TrustedID credit protection company will be an effective and trustworthy source to guard against

1 identity theft.

2 30. Plaintiffs are concerned that they will have to “look over their shoulder”
3 for the rest of their lives, spending time constantly monitoring their credit and
4 banking accounts for fraudulent activity, as a result of the Equifax data breach. As a
5 direct result of Equifax’s conduct, Plaintiffs are worried, fearful, frustrated,
6 distressed, and angry.

7 **Equifax Was Asleep at the Wheel**

8 31. Upon information and belief, Equifax failed to develop, implement, and
9 maintain a comprehensive information security program with administrative, technical,
10 and physical safeguards that were appropriate to its size and complexity, the nature
11 and scope of [its] activities, and the sensitivity of any customer information at issue.
12 This includes, but is not limited to, Equifax’s failure to implement and maintain
13 adequate data security practices to safeguard Class Members’ PII; (b) failing to detect
14 the Data Breach in a timely manner; and (c) failing to disclose that Defendants’ data
15 security practices were inadequate to safeguard Class Members’ PII.

16 32. The Data Breach was a direct result of Equifax’s failure to implement
17 adequate security measures to safeguard consumers’ PII and willfully ignored
18 known weaknesses in its data security, including prior hacks into its information
19 systems. Unauthorized parties routinely attempt to gain access to and steal personal
20 information from networks and information systems—especially from entities such as
21 Equifax, which are known to possess a large number of individuals’ valuable personal
22 and financial information.

23 33. Upon information and belief, Equifax also failed to develop and
24 implement a risk-based response program to address incidents of unauthorized access
25 to customer information in customer information systems. This includes, but is not
26 limited to, Equifax’s failure to notify appropriate regulatory agencies, law
27 enforcement, and the affected individuals themselves of the Data Breach in a timely
28 and adequate manner.

1 34. Equifax failed to notify affected consumers promptly after it became
2 aware of unauthorized access to sensitive customer information, and sat on the
3 knowledge for more than a month. As of the date of this filing, Equifax has continued
4 to fail to communicate the Data Breach directly with Plaintiffs and Class Members to
5 date.

6 35. Equifax also has failed to properly guard against the barrage of identity
7 theft which is surely to follow. While Equifax offers free credit protection for a year,
8 Plaintiffs and members of the class will require a *lifetime* of credit protection. Equifax
9 is bound to profit generously by the tens of millions of consumers who will begin
10 paying Equifax to continue credit protection at the end of their free year.

11 **Equifax's Failure to Protect PII is Actionable**

12 36. According to the FTC, the failure to employ reasonable and appropriate
13 measures to protect against unauthorized access to confidential consumer data
14 constitutes an unfair act or practices prohibited by Section 5 of the FTC Act, 15 U.S.C.
15 § 45. 41.

16 37. In 2007, the FTC published guidelines which establish reasonable data
17 security practices for businesses. The guidelines note businesses should protect the
18 personal customer information that they keep; properly dispose of personal
19 information that is no longer needed; encrypt information stored on computer
20 networks; understand their network's vulnerabilities; and implement policies for
21 installing vender-approved patches to correct security problems. The guidelines also
22 recommend that businesses consider using an intrusion detection system to expose a
23 breach as soon as it occurs; monitor all incoming traffic for activity indicating
24 someone may be trying to hack the system; watch for large amounts of data being
25 transmitted from the system; and have a response plan ready in the event of a breach.

26 38. The FTC also published a document entitled "FTC Facts for Business"
27 which highlights the importance of having a data security plan, regularly assessing
28 risks to computer systems, and implementing safeguards to control such risks.

1 39. The FTC has issued orders against businesses that fail to employ
2 reasonable measures to secure customer data. These orders provide further guidance to
3 businesses with regard to their data security obligations.

4 40. By failing to have reasonable data security measures in place, Equifax
5 engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

6 41. By failing to have reasonable data security measures in place, Equifax
7 caused harm to Plaintiffs and Class Members as aforementioned.

8 CLASS ACTION ALLEGATIONS

9 42. Plaintiffs bring all claims as class claims under Federal Rules of Civil
10 Procedure, Rule 23(b)(1), (b)(2), (b)(3), and (c)(4).

11 43. **Nationwide Class**: Plaintiffs bring their Negligence, Negligence Per Se,
12 FCRA, Declaratory and Injunctive Relief Claims (Counts I, II and V, VII & VIII) on
13 behalf of a proposed nationwide class (“Nationwide Class”), defined as follows:

14 **I. All natural persons and entities in the United States
15 whose personally identifiable information was acquired
16 by unauthorized persons in the data breach announced
17 by Equifax on September 7, 2017.**

18 44. **California Subclass**: Plaintiffs bring their State Data-breach-notification
19 claim, Privacy, and UCL claims (Counts II, IV & VI) on behalf of a separate statewide
20 subclass, defined as follows:

21 **II. All natural persons and entities in California whose
22 personally identifiable information was acquired by
23 unauthorized persons in the data breach announced by
24 Equifax on September 7, 2017.**

25 45. Collectively, all these persons will be referred to as “Class Members.”
26 Plaintiffs represent, and are members of the Class. Excluded from the Class are
27 Equifax and any entities in which Equifax has a controlling interest, Equifax’s agents
28 and employees, any Judge to whom this action is assigned and any member of such
Judge’s staff and immediate family, and claims for personal injury, wrongful death
and/or emotional distress.

1 46. Plaintiffs reserve the right to amend or modify the class definition after
2 discovery has been conducted.

3 **Certification of the Proposed Classes Is Appropriate**

4 47. Each of the proposed Classes meets the requirements of Fed. R. Civ. P.
5 23(a) (b)(1), (b)(2), (b)(3) and (c)(4).

6 48. **Numerosity.** Plaintiffs does not know the exact number of members in
7 the Class or the subclasses, but based upon Defendant's September 7, 2017 press
8 release, the Class consists of approximately 143 million individuals. The joinder of all
9 Class Members is impracticable due to the size and relatively modest value of each
10 individual claim. The disposition of the claims in a class action will provide
11 substantial benefit to the parties and the Court in avoiding a multiplicity of identical
12 suits. The Class can be identified easily through records maintained by Equifax.

13 49. **Commonality.** There are well-defined, nearly identical, questions of law
14 and fact affecting the Class. The questions of law and fact involving the class claims
15 predominate over questions that may affect individual Class Members. Those common
16 questions of law and fact include, but are not limited to, the following:

- 17 a. Whether Equifax failed to adequately safeguard Plaintiffs' and the
18 Classes' Personal Information;
- 19 b. Whether Equifax failed to protect Plaintiffs' and the Classes' Personal
20 Information, as promised;
- 21 c. Whether Defendants' computer system systems and data security
22 practices used to protect Plaintiffs' and the Classes' Personal Information
23 violated federal, state and local laws, or Defendants' duties;
- 24 d. Whether Defendants engaged in unfair, unlawful, or deceptive practices
25 by failing to safeguard Plaintiffs' and the Classes' Personal Information
26 properly and/or as promised;
- 27 e. Whether Defendants violated the consumer protection statutes, data
28 breach notification statutes applicable to Plaintiffs and each of the

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

Classes;

- f. Whether Defendants failed to notify Plaintiffs and members of the Classes about the Equifax Breach on a timely basis after the Equifax Data Breach was discovered, and whether its failure to notify consumers promptly resulted in additional harm.
- g. Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Classes' Personal Information;
- h. Whether Defendants should retain the money paid by Plaintiffs and members of each of the Classes to protect their Personal Information beyond the free year offered by Equifax;
- i. Whether Plaintiffs and Class Members should receive more than a year of credit protection at no cost.
- j. Whether Plaintiffs and the members of the Classes are entitled to damages as a result of Defendants' wrongful conduct;
- k. Whether Plaintiffs and the members of the Classes are entitled to restitution as a result of Defendants' wrongful conduct;
- l. What equitable relief is appropriate to redress Defendants' wrongful conduct; and
- m. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Classes.

50. **Typicality.** All Plaintiffs' claims are typical of the claims of the Nationwide Class, and each of Plaintiffs' claims are typical of the claims of the Statewide Subclass.

51. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Nationwide Class and Statewide Subclasses. Plaintiffs have no interests that are adverse to, or in conflict with, the Class Members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient

1 resources to prosecute this action vigorously.

2 52. **Superiority.** A class action is the superior method for the fair and
3 efficient adjudication of this controversy. The interests of Class Members in
4 individually controlling an individual action are small.

5 53. Defendant has acted on grounds generally applicable to the Class, thereby
6 making final injunctive relief and corresponding declaratory relief with respect to the
7 Class as a whole appropriate.

8 54. **Injunctive and /or Declaratory Relief:** In addition, Defendants have
9 acted and/or refused to act on grounds that apply generally to the Nationwide and
10 Statewide Subclass, making injunctive and/or declaratory relief appropriate with
11 respect to the classes under Federal Rule of Civil Procedure 23(b)(2). Defendants
12 continue to (1) maintain the PII of Class Members, and (2) fail to adequately protect
13 their PII.

14 55. **Certification of Particular Issues:** In the alternative, the Nationwide and
15 Statewide Subclass may be maintained as class actions with respect to particular
16 issues, in accordance with Fed. R. Civ. P. 23(c)(4).

17
18 **CAUSES OF ACTION**

19 **COUNT I**
20 **NEGLIGENCE**

21 **(On Behalf of the Nationwide Class and the Statewide Subclass)**

22 56. Plaintiffs incorporate all prior paragraphs as if fully set forth here.

23 57. Equifax owed a duty to Plaintiffs and Class Members, arising from the
24 sensitivity of the information and the foreseeability of its data safety shortcomings
25 resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive
26 personal information. This duty included, among other things, designing, maintaining,
27 monitoring, and testing Equifax's security systems, protocols, and practices to ensure
28 that Class Members' information adequately secured from unauthorized access.

58. Equifax's privacy policy acknowledged Equifax's duty to adequately

1 protect Class Member's PII.

2 59. Equifax owed a duty to Class Members to implement intrusion detection
3 processes that would detect a data breach in a timely manner.

4 60. Equifax also had a duty to delete any PII that was no longer needed to
5 serve client needs.

6 61. Equifax owed a duty to disclose the material fact that its data security
7 practices were inadequate in order to safeguard Class Member's PII.

8 62. Equifax also had independent duties under state laws that required Equifax
9 to reasonably safeguard Plaintiffs' and Class Members' PII and promptly notify them
10 about the Data Breach.

11 63. Equifax had a special relationship with Plaintiffs and Class Members from
12 being entrusted with their PII, which provided an independent duty of care. Plaintiff's
13 and other Class Members' willingness to entrust Equifax with their PII was predicated
14 on the understanding that Equifax would take adequate security precautions.
15 Moreover, Equifax had the ability to protect its systems and Class Members' PII from
16 attack.

17 64. Equifax's role to utilize and purportedly safeguard Plaintiffs' and Class
18 Members' PII presents unique circumstances requiring a reallocation of risk.

19 65. Equifax breached its duties by, among other things: (a) failing to
20 implement and maintain adequate data security practices to safeguard Class Member's
21 PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that
22 Defendants' data security practices were inadequate to safeguard Class Member's PII;
23 and (d) failing to provided adequate and timely notice of the breach.

24 66. But for Equifax's breach of its duties, Class Member's PII would not have
25 been accessed by unauthorized individuals.

26 67. Plaintiffs and Class Members were foreseeable victims of Equifax's
27 inadequate data security practices. Equifax knew or should have known that a breach
28 of its data security systems would cause damages to Plaintiffs and the Class Members.

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

68. Equifax’s negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs’ and the Nationwide Class Member’s PII and consumer reports.

69. As a result of Equifax’s willful failure to prevent the Data Breach, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures, such as Plaintiffs’ purchases of credit protection services and insurance. The unauthorized acquisition of Plaintiffs’ and Class Member’s PII has also diminished the value of their PII.

70. The damages to Plaintiffs and the Class Members were a proximate, reasonably foreseeable result of Equifax’s breaches of its duties.

71. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE
(On behalf of the Nationwide Class and the Statewide Subclass)

72. Plaintiffs incorporates all prior paragraphs as if fully set forth herein.

73. Section 5 of the Federal Trade commission Act (“FTC Act”), 15 U.S.C. § prohibits “unfair...practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by businesses such as Equifax of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form the basis of Equifax’s duty.

74. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Equifax’s conduct was particularly unreasonable given the nature and amount of PII it

1 obtained and stored and the foreseeable consequences of a data breach in their
2 systems, including specifically the immense damages that would result to consumers.

3 75. Equifax's violation of Section 5 of the FTC Act constitutes negligence per
4 se.

5 76. Members of the Class and Subclass are within the class of persons Section
6 5 of the FTC Act was intended to protect as they are individuals engaged in trade and
7 commerce, and bear the risk associated with defendant's failure to properly secure
8 their PII.

9 77. Moreover, the harm that has occurred is the type of harm the FTC Act was
10 intended to guard against. The FTC has pursued over fifty enforcement actions against
11 businesses which, as a result of their failure to employ reasonable data security
12 measures and avoid unfair and deceptive practices, have put consumers' personal data
13 at unreasonable risk, causing the same harm suffered by Class Members.

14 78. Equifax was further required under the Gramm-Leach-Bliley Act
15 ("GLBA") to satisfy certain standards relating to administrative, technical, and
16 physical safeguards: (1) to insure the security and confidentiality of customer records
17 and information; (2) to protect against any anticipated threats or hazards to the security
18 or integrity of such records; and (3) to protect against unauthorized access to or use of
19 such records or information which could result in substantial harm or inconvenience to
20 any customer.

21 79. In order to satisfy their obligations under the GLBA, Equifax was also
22 required to "develop, implement, and maintain a comprehensive information security
23 program that is [1] written in one or more readily accessible parts and [2] contains
24 administrative, technical, and physical safeguards that are appropriate to [its] size and
25 complexity, the nature and scope of [its] activities, and the sensitivity of any customer
26 information at issue." See 16 C.F.R. § 314.4.

27 80. In addition, under the Interagency Guidelines Establishing Information
28 Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to

1 “develop and implement a risk-based response program to address incidents of
2 unauthorized access to customer information in customer information systems.” *See*
3 *Id.*

4 81. Further, when Equifax became aware of “unauthorized access to sensitive
5 customer information,” it should have “conduct[ed] a reasonable investigation to
6 promptly determine the likelihood that the information has been or will be misused”
7 and “notif[ied] the affected customer[s] as soon as possible.” *See Id.*

8 82. Equifax violated by GLBA by failing to “develop, implement, and
9 maintain a comprehensive information security program” with “administrative,
10 technical, and physical safeguards” that were “appropriate to [its] size and complexity,
11 the nature and scope of [its] activities, and the sensitivity of any customer information
12 at issue.” This includes, but is not limited to, Equifax’s failure to implement and
13 maintain adequate data security practices to safeguard Class Member’s PII; (b) failing
14 to detect the Data Breach in a timely manner; and (c) failing to disclose that
15 Defendants’ data security practices were inadequate to safeguard Class Members’ PII.

16 83. Equifax also violated the GLBA by failing to “develop and implement a
17 risk-based response program to address incidents of unauthorized access to customer
18 information in customer information systems.” This includes, but is not limited to,
19 Equifax’s failure to notify appropriate regulatory agencies, law enforcement, and the
20 affected individuals themselves of the Data Breach in a timely and adequate manner.

21 84. Equifax also violated by the GLBA by failing to notify affected customers
22 as soon as possible after it became aware of unauthorized access to sensitive customer
23 information.

24 85. Plaintiffs and Class Members were foreseeable victims of Equifax’s
25 violations of the FTC Act and GLBA. Equifax knew or should have known that its
26 failure to take reasonable measures to prevent a breach of its data security systems, and
27 failure to timely and adequately notify the appropriate regulatory authorities, law
28 enforcement, and Class Members themselves would cause damages to Class Members.

1 86. Defendants’ failure to comply with the applicable laws and regulations,
2 including the FTC Act and GLBA, constitute negligence per se.

3 87. But for Equifax’s violation of the applicable laws and regulations,
4 Plaintiffs and Class Members’ PII would not have been accessed by unauthorized
5 individuals.

6 88. As a result of Equifax’s failure to comply with applicable laws and
7 regulations, Plaintiffs and Class Members suffered injury, which includes but is not
8 limited to exposure to a heightened, imminent risk of fraud, identity theft, and
9 financial harm. Plaintiffs and Class Members must more closely monitor their
10 financial accounts and credit histories to guard against identity theft. Class Members
11 also have incurred, and will continue to incur on an indefinite basis, out-of-pocket
12 costs for obtaining credit reports, credit freezes, credit monitoring services, and other
13 protective measures to deter or detect identity theft. The unauthorized acquisition of
14 Plaintiffs and Class Members’ PII has also diminished the value of the PII.

15 89. The damages to Plaintiffs and the Class Members were a proximate,
16 reasonably foreseeable result of Equifax’s breaches of the applicable laws and
17 regulations.

18 90. Therefore, Plaintiffs and Class Members are entitled to damages in an
19 amount to be proven at trial.

20 **COUNT III**
21 **VIOLATION OF THE CALIFORNIA CONSUMER**
22 **RECORDS ACT, CIVIL CODE § 1798.81 *ET SEQ.***
23 **(On Behalf of the Statewide Subclass)**

24 91. Plaintiffs incorporates all prior paragraphs as if fully set forth herein.

25 92. Plaintiffs brings this cause of action on behalf of the California Class
26 whose PII is maintained by Equifax and/or that was compromised in the Data Breach
27 announced on September 7, 2017.

28 93. “[T]o ensure that personal information about California residents is
protected,” the California Legislature enacted California Customer Records Act. This
statute states that any business that “owns or licenses personal information about a

1 California resident shall implement and maintain reasonable security procedures and
2 practices appropriate to the nature of the information, to protect the personal
3 information from unauthorized access, destruction, use, modification, or disclosure.”
4 Civil Code section 1798.81.5.

5 94. Equifax is a “business” within the meaning of Civil Code section
6 1798.80(a).

7 95. Plaintiffs and members of the class are “individual[s]” within the
8 meaning of the Civil Code section 1798.80(d). Pursuant to Civil Code sections
9 1798.80(e) and 1798.81.5(d)(1)(C), “personal information” includes an individual’s
10 name, Social Security number, driver’s license or state identification card number,
11 debit card and credit card information, medical information, or health insurance
12 information. “Personal information” under Civil Code section 1798.80(e) also
13 includes address, telephone number, passport number, education, employment,
14 employment history, or health insurance information.

15 96. The breach of the personal data of tens of millions consumers constitutes
16 a “breach of the security system” of Equifax pursuant to Civil Code section
17 1798.82(g).

18 97. By failing to implement reasonable measures to protect consumers’
19 personal data, Equifax violated Civil Code section 1798.81.5.

20 98. California Civil Code § 1798.82 requires that any business that retains
21 personal information from its customers (including personal identification data) must
22 promptly and "in the most expedient time possible and without unreasonable delay"
23 disclose any breach of the security of the system containing such retained data.
24 California Civ. Code § 1798.82 also requires that any notice convey specific
25 information about what happened, what specific information was disclosed, what the
26 institution maintaining the information is doing about the unauthorized disclosure,
27 and how an affected customer can obtain more information about the unauthorized
28 disclosure.

1 99. Plaintiffs, on their own behalf and on behalf of the Statewide Subclass,
2 allege that Defendants failed to disclose what specific information was disclosed,
3 what Equifax did or is doing about the unauthorized disclosure of Plaintiffs and Class
4 members' PII, how Plaintiffs and the Class members' could obtain more information
5 about the unauthorized disclosure, and unreasonably delayed in disclosing to
6 Plaintiffs and the Subclass the breach in security of PII of Plaintiffs and the Class
7 when Defendant knew such information had been acquired by an unauthorized
8 person or persons.

9 100. Equifax's September 7, 2017 press release fails to satisfy the basic notice
10 requirements of Cal. Civ. Code § 1798.82(d).

11 101. Plaintiffs, on their own behalf and on behalf of the Class, allege upon
12 information and belief that no law enforcement agency determined or instructed any
13 Defendant that notifications of Plaintiffs or the Class would impede a criminal
14 investigation.

15 102. As a direct and proximate result of the acts and omissions by Defendants
16 described herein, Plaintiffs and the Class have suffered and/or will suffer significant
17 economic harm including the costs associated with, *inter alia*: (a) their purchase of
18 sufficient identity-theft-prevention and credit monitoring services; (b) lower credit
19 scores which have resulted or will result from, among other things, the large number
20 of credit bureau inquiries associated with the actual and attempted thefts of their
21 identities; (c) their purchase of credit-repair services; (d) their time spent monitoring
22 their credit reports by nationwide consumer credit agencies; (e) their time spent
23 otherwise dealing with the numerous adverse effects of identity information theft;
24 and/or (g) all other forms of economic harm and actual damages arising out of the
25 theft of their confidential information.

26 103. As a direct and proximate result of the acts and omissions by Defendants
27 described herein, Plaintiffs and the Subclass have suffered and/or will suffer
28 significant non-economic harm including, *inter alia*, fear, anxiety and stress.

COUNT IV
VIOLATION OF ARTICLE I, §1 OF THE CALIFORNIA
CONSTITUTION (RIGHT TO PRIVACY)
(On Behalf of the Statewide Subclass)

1
2
3
4 104. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

5 105. California law establishes a right to privacy in individuals pursuant to,
6 among other things, Article I, section 1 of the California Constitution and common
7 law. To establish a claim for violation of the Constitutional right to privacy, a
8 claimant need only establish: (a) a legally protected privacy interest; (b) a reasonable
9 expectation of privacy under the circumstances, and (c) a serious invasion of the
10 privacy interest. To establish a claim for invasion of privacy based on the public
11 disclosure of private facts, a claimant need only establish: (a) public disclosure of
12 private facts; (b) that would be offensive and objectionable to a reasonable person;
13 and (c) which is not of legitimate public concern.

14 106. Plaintiffs and the Class members have a legally protected privacy interest
15 in their PII. Plaintiffs and the Class members had a reasonable expectation of privacy
16 under the circumstances. Further, Defendant's conduct, omissions and/or negligence
17 constitutes a serious invasion of the privacy interests of Plaintiffs and the Class
18 members.

19 107. Similarly, Plaintiffs and the Class members' PII was publicly disclosed
20 by Defendant. Defendant's conduct, omissions and/or negligence is offensive and
21 objectionable to a reasonable person. Further, the stolen information is not of
22 legitimate public concern. Defendant's acts and/or omissions were unauthorized.

23 108. As a direct and proximate result of Defendants' misconduct as set forth
24 herein, Plaintiffs and the Class members have suffered harm and will continue to
25 suffer harm, including but not limited to loss of and invasion of privacy, loss of
26 property, and loss of control of their medical information and personal financial
27 information.

28 109. As a direct and proximate result of the acts and omissions by Defendant
described herein, Plaintiffs and the Class have suffered and/or will suffer significant

1 economic harm including the costs associated with, *inter alia*: (a) their purchase of
2 sufficient identity-theft-prevention and credit monitoring services; (b) lower credit
3 scores which have resulted or will result from, among other things, the large number
4 of credit bureau inquiries associated with the actual and attempted thefts of their
5 identities; (c) their purchase of credit-repair services; (d) their time spent monitoring
6 their credit reports by nationwide consumer credit agencies; (e) their purchase of
7 home security services such as ADT®; (f) their time spent otherwise dealing with the
8 numerous adverse effects of identity information theft; and/or (g) all other forms of
9 economic harm and actual damages arising out of the theft of their confidential
10 information.

11 110. As a direct and proximate result of the acts and omissions by Defendants
12 described herein, Plaintiffs and the Class have suffered and/or will suffer significant
13 non-economic harm including, *inter alia*, fear, anxiety and stress.

14 **COUNT V**
15 **DECLARATORY AND INJUNCTIVE RELIEF**
16 **(On behalf of the Nationwide Class and the Statewide Subclass)**

17 111. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

18 112. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 et seq., this Court
19 is authorized to enter a judgment declaring the rights and legal relations of the parties
20 and grant further necessary relief. Furthermore, the Court has broad authority to
21 restrain acts, such as here, which are tortuous and which violate the terms of the
22 federal and state statutes described in this complaint.

23 113. An actual controversy has arisen in the wake of Equifax's data breach
24 regarding its common law and other duties to reasonably safeguard individuals PII.
25 Plaintiffs allege that Equifax's data security measures were inadequate and remain
26 inadequate.

27 114. Pursuant to its authority under the Declaratory Judgment Act, this Court
28 should enter a judgment declaring, among other things, the following:

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

- a. Equifax owed and continues to owe a legal duty to secure Class Members’ personal and financial information and to notify Class Members of a data breach under the common law, Section 5 of the FTC Act and GLBA;
- b. Equifax breached and continues to breach this legal duty by failing to employ reasonable security measures to secure Class Members’ PII;
- c. Equifax’s breach of its legal duty proximately caused the data breach which it announced on September 7, 2017;
- d. Equifax’s continued failure to disclose exactly the scope of the data breach, and the individuals effected by the breach makes it impossible for class members to take appropriate measures to mitigate the risk of future identity theft;
- e. Equifax’s remedy to protect Class Members by offering consumers a free year of credit protection is insufficient.

115. The Court also should issue corresponding injunctive relief requiring Equifax to employ adequate security protocols to protect the PII of Class Members in its possession. Specifically, this injunction should, among other things direct Equifax to:

- a. utilize industry standard secure default password and pin combinations in protecting individuals’ PII;
- b. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;
- c. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;
- d. regularly test its system for security vulnerabilities, consistent with industry standards;
- e. immediately notify all Class Members of the data breach, and the scope

1 of PII that was disclosed;

2 f. provide Class Members more than one free year of free credit
3 protection.

4 116. If an injunction is not issued, Class Members will suffer irreparable injury
5 and lack an adequate remedy in the event of another data breach, at Equifax. The risk
6 of another such breach is real, immediate, and substantial. If another breach at Equifax
7 occurs, Class members will not have an adequate remedy at law because many of the
8 resulting injuries are not readily quantified and they will be forced to bring multiple
9 lawsuits to rectify the same conduct.

10 117. The hardship to the Class if an injunction does not issue exceeds the
11 hardship to Equifax if an injunction is issued. Among other things, if another data
12 breach occurs at Equifax, the class will likely incur further risk of identity theft and
13 fraudulent use of their PII. On the other hand, the cost to Equifax of complying with an
14 injunction by employing reasonable data security and notice measures is relatively
15 minimal, and Equifax has a pre-existing legal obligation to employ such measures.

16 118. Issuance of the requested injunction will not disserve the public interest.
17 To the contrary, such an injunction would benefit the public by preventing another data
18 breach at Equifax, thus eliminating the injuries that would result to Class Members and
19 others whose PII Equifax later obtains whose information would be compromised.

20

21 **COUNT VI**
22 **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW,**
23 **BUS. & PROF. CODE SECTION 17200 *ET SEQ.***
(On Behalf of the Statewide Class)

24 119. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

25 120. Defendants' conduct and violations of law constitute unlawful conduct
26 within the meaning of the UCL.

27 121. Defendant violated the CCRA, as alleged herein by failing to safeguard,
28 and disclosing Plaintiffs' and Class Members' PII, and failing to provide adequate and

1 timely notice of the disclosure.

2 122. Defendant willfully and negligently violated the FCRA, as alleged
3 herein.

4 123. Defendant has violated Section 5 of the FTC ACT as alleged herein.

5 124. Defendant violated the UCL by engaging in unfair business practices by
6 failing to implement appropriate procedures to guard against the release of Class
7 Members PPI.

8 125. As a direct result of Defendant's violation of the UCL, Plaintiffs incurred
9 a distinct financial injury by being forced to purchase credit protection to ward off
10 future identity thieves.

11 126. Pursuant to the Business & Professions Code § 17203, Plaintiffs and the
12 Class seek an order of this Court for equitable and/or injunctive relief in the form of
13 an order: (a) enjoining Defendants from continuing their unlawful practices described
14 herein; (b) directing Defendant to notify, with Court supervision, all Class members in
15 full of the actual information stolen and/or potential theft of their identities as a result
16 of the events underlying this class action; (c) directing Defendant to implement
17 security measures regarding private information that comply with the law; ; and (d)
18 requiring Defendant to provide for Plaintiff's and the Class Members': (i) a lifetime
19 of adequate identity-theft-prevention and credit monitoring services; (ii) credit repair
20 services; (iii) sufficient identity theft insurance; (iv) home security services; and for
21 (v) all other forms of restitution.

22
23 **COUNT VII**
24 **WILLFUL VIOLATION OF THE FAIR CREDIT**
25 **REPORTING ACT, 15 U.S.C. § 1681A(C).**
26 **(On behalf of the Nationwide Class)**

27 127. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

28 128. As individuals, Plaintiffs and Class member are consumers entitled to the
protections of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681a(c). Under
the FCRA, a "consumer reporting agency" is defined as "any person which, for

1 monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or
2 in part in the practice of assembling or evaluating consumer credit information or other
3 information on consumers for the purpose of furnishing consumer reports to third
4 parties” 15 U.S.C. § 1681a(f). Equifax is a consumer reporting agency under the
5 FCRA because, for monetary fees, it regularly engages in the practice of assembling or
6 evaluating consumer credit information or other information on consumers for the
7 purpose of furnishing consumer reports to third parties.

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

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

24 131. As a consumer reporting agency, Equifax may only furnish a consumer
25 report under the limited circumstances set forth in 15 U.S.C. § 1681b, “and no other.”
26 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit
27 credit reporting agencies to furnish consumer reports to unauthorized or unknown
28 entities, or computer hackers such as those who accessed the Nationwide Class

1 members' PII.

2 132. Equifax violated § 1681b by furnishing consumer reports to unauthorized
3 or unknown entities or computer hackers, as detailed above. Equifax furnished
4 Plaintiffs and the Nationwide Class members' consumer reports by disclosing their
5 consumer reports to unauthorized entities and computer hackers; allowing
6 unauthorized entities and computer hackers to access their consumer reports;
7 knowingly and/or recklessly failing to take security measures that would prevent
8 unauthorized entities or computer hackers from accessing their consumer reports;
9 and/or failing to take reasonable security measures that would prevent unauthorized
10 entities or computer hackers from accessing their consumer reports.

11 133. The Federal Trade Commission ("FTC") has pursued enforcement actions
12 against consumer reporting agencies under the FCRA for failing to "take adequate
13 measures to fulfill their obligations to protect information contained in consumer
14 reports, as required by the" FCRA, in connection with data breaches.

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

25 135. In addition, Equifax acted willfully and recklessly because it knew or
26 should have known about its legal obligations regarding data security and data breaches
27 under the FCRA. These obligations are well established in the plain language of the
28 FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.,* 55 Fed.

1 Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16
2 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available
3 these and other substantial written materials that apprised them of their duties under the
4 FCRA. Any reasonable consumer reporting agency knows or should know about these
5 requirements. Despite knowing of these legal obligations, Equifax acted consciously in
6 breaching known duties regarding data security and data breaches and depriving
7 Plaintiffs and other members of the classes of their rights under the FCRA. Equifax's
8 willful and/or reckless conduct provided a means for unauthorized intruders to obtain
9 and misuse Plaintiffs' and Nationwide Class members' personal information for no
10 permissible purposes under the FCRA.

11 136. Plaintiffs and the Nationwide Class members have been damaged by
12 Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and
13 each of the Nationwide Class members are entitled to recover "any actual damages
14 sustained by the consumer . . . or damages of not less than \$100 and not more than
15 \$1,000." 15 U.S.C. § 1681n(a)(1)(A).

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

19
20 **COUNT VIII**
21 **NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**
22 **(On Behalf of the Nationwide Class)**

23 138. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

24 139. Equifax was negligent in failing to maintain reasonable procedures
25 designed to limit the furnishing of consumer reports to the purposes outlined under
26 section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable
27 procedures is supported by, among other things, former employees' admissions that
28 Equifax's data security practices have deteriorated in recent years, and Equifax's
numerous other data breaches in the past. Further, as an enterprise claiming to be an

1 industry leader in data breach prevention, Equifax was well aware of the importance of
2 the measures organizations should take to prevent data breaches yet failed to take them.

3 140. Equifax’s negligent conduct provided a means for unauthorized intruders
4 to obtain Plaintiffs’ and the Nationwide Class members’ PII and consumer reports for
5 no permissible purposes under the FCRA.

6 141. Plaintiffs and the Nationwide Class member have been damaged by
7 Equifax’s negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of
8 the Nationwide Class member are entitled to recover “any actual damages sustained by
9 the consumer.” 15 U.S.C. § 1681o(a)(1).

10 142. Plaintiffs and the Nationwide Class member are also entitled to recover
11 their costs of the action, as well as reasonable attorneys’ fees. 15 U.S.C. § 1681o(a)(2).

12
13 **PRAYER FOR RELIEF**

14 WHEREFORE, Plaintiffs respectfully request that the Court grant Plaintiffs
15 and Class Members the following relief against Defendant:

- 16 A. An order certifying this action as a class action under Federal Rule of
17 Civil Procedure 23, defining the Class and Subclass requested herein,
18 appointing the undersigned as Class Counsel, and finding that Plaintiffs
19 are proper representatives of the Class and Subclass requested herein;
- 20 B. Injunctive relief requiring Defendants to (1) strengthen their data
21 security systems that maintain PII to comply with the, the applicable
22 state laws alleged herein and best practices under industry standards;
23 (2) engage third-party auditors and internal personnel to conduct
24 security testing and audits on Defendants’ systems on a periodic basis;
25 (3) promptly correct any problems or issues detected by such audits
26 and testing; and (4) routinely and continually conduct training to
27 inform internal security personnel how to prevent, identify and contain
28 a breach, and how to appropriately respond;

- 1 C. An order requiring Defendants to pay all costs associated with Class
2 notice and administration of Class-wide relief;
- 3 D. An award to Plaintiffs and all Class (and Subclass) Members of
4 compensatory, consequential, incidental, and statutory damages,
5 restitution, and disgorgement, in an amount to be determined at trial;
- 6 E. An award to Plaintiffs and all Class (and Subclass) Members of a
7 lifetime of credit monitoring and identity theft protection services
8 provided by an entity other than Defendant;
- 9 F. An award of attorneys' fees, costs, and expenses, as provided by law or
10 equity;
- 11 G. An order Requiring Defendants to pay pre-judgment and post-
12 judgment interest, as provided by law or equity; and
- 13 H. Such other or further relief as the Court may allow.
- 14

15 **DEMAND FOR JURY TRIAL**

16 Plaintiffs demand a trial by jury of all issues in this action so triable of right.

17

18 Dated: September 11, 2017

Respectfully submitted,

19
20 **COAST LAW GROUP LLP**

21 By: s/ Helen I. Zeldes

Helen I. Zeldes, Esq. (SBN 220051)

22 E-mail: helen@coastlaw.com

23 **HUSSIN LAW**

24 BY: s/ Tammy Gruder Hussin

Tammy Gruder Hussin (SBN 155290)

25
26
27 Counsel for Plaintiffs Christopher Tanks,
28 Brittany Dixon and the Putative Class

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Christopher Tanks and Brittany Dixon

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

(c) Attorneys (Firm Name, Address, and Telephone Number) Helen I. Zeldes, Coast Law Group 1140 S. Coast Hwy. 101, Encinitas CA 92024

DEFENDANTS

Equifax, Inc.; and DOES 1-10

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

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

Attorneys (If Known)

'17CV1832 BAS BLM

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

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

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

- Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, PTF DEF, 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)

Table with columns: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, TORTS, PRISONER PETITIONS, LABOR, IMMIGRATION, FORFEITURE/PENALTY, SOCIAL SECURITY, FEDERAL TAX SUITS, BANKRUPTCY, OTHER STATUTES. Includes various legal categories like Personal Injury, Property Damage, Labor, etc.

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): Fair Credit Reporting Act, 15 USC section 1681(a)(c)
Brief description of cause: Negligent data breach by defendant resulting in violations of the FCRA

VII. REQUESTED IN COMPLAINT:

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

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE DOCKET NUMBER

DATE SIGNATURE OF ATTORNEY OF RECORD

s/ Helen I. Zeldes

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 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 by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. 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 Rule 8(a), F.R.Cv.P., 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.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 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.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 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 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 there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN 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 Rule 23, F.R.Cv.P.
 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 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.