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

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

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

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

CHRISTOPHER TANKS and BRITTANY DIXON, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

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

Defendants.

Civil Case No.: **'17CV1832 BAS BLM**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

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

NATURE OF THE ACTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

JURISDICTION AND VENUE

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

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

PARTIES

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

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

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

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

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

FACTUAL ALLEGATIONS

Equifax's Unprecedented Data Breach

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

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

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

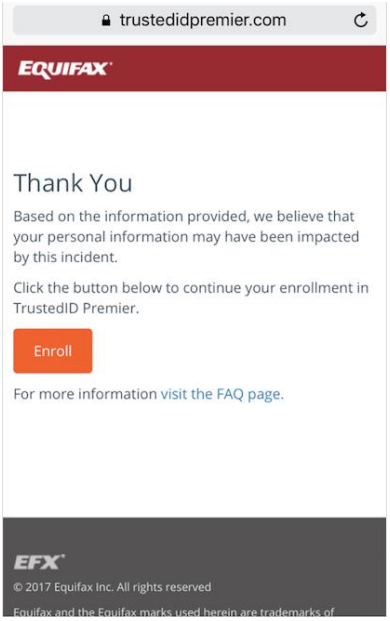
22. Plaintiffs and Class Members have suffered harm as a result of Equifax's negligence and willful ignorance in the form of additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the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

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

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

Plaintiffs' PII Was Fraudulently Used During the Data Breach

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

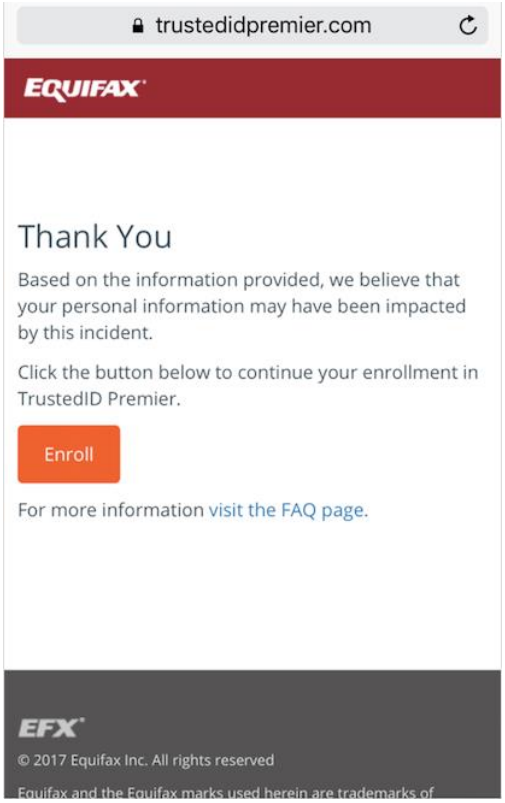


25. On or about the last week of July of 2017 – during the time frame Equifax disclosed its massive data breach occurred -- Mr. Tanks learned that his identity had been stolen and someone had run an unauthorized $25.00 charge through his bank account. Mr. Tanks filed a fraud claim with his bank and was issued a new debit card.

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

[1] http://www.equifax.com/privacy/

data breach and received this message:



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

identity theft.

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

Equifax Was Asleep at the Wheel

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

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

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

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

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

Equifax's Failure to Protect PII is Actionable

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

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

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

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

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

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

CLASS ACTION ALLEGATIONS

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

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

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

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

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

45. Collectively, all these persons will be referred to as "Class Members." Plaintiffs represent, and are members of the Class. Excluded from the Class are Equifax and any entities in which Equifax has a controlling interest, Equifax's agents 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.

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

Certification of the Proposed Classes Is Appropriate

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

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

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

a. Whether Equifax failed to adequately safeguard Plaintiffs' and the Classes' Personal Information;

b. Whether Equifax failed to protect Plaintiffs' and the Classes' Personal Information, as promised;

c. Whether Defendants' computer system systems and data security practices used to protect Plaintiffs' and the Classes' Personal Information violated federal, state and local laws, or Defendants' duties;

d. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Personal Information properly and/or as promised;

e. Whether Defendants violated the consumer protection statutes, data breach notification statutes applicable to Plaintiffs and each of the

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

resources to prosecute this action vigorously.

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

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

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

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class and the Statewide Subclass)

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

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

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

protect Class Member's PII.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See Id*.

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

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

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

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

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

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

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

88. As a result of Equifax's failure to comply with applicable laws and regulations, 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. 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 to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class Members' PII has also diminished the value of the PII.

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

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

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

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

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

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

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

94. Equifax is a "business" within the meaning of Civil Code section 1798.80(a).

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

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

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

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

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

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

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

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

103. As a direct and proximate result of the acts and omissions by Defendants described herein, Plaintiffs and the Sucblass have suffered and/or will suffer 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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

of PII that was disclosed;

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

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

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

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

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

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

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

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

timely notice of the disclosure.

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

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

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

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

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

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

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

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

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

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

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

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

members' PII.

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

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

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

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

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

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

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

COUNT VIII
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On Behalf of the Nationwide Class)

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

139. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that 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

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

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

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

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

PRAYER FOR RELIEF

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

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and Subclass requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Class and Subclass requested herein;

B. Injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain PII to comply with the, the applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

C. An order requiring Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiffs and all Class (and Subclass) Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiffs and all Class (and Subclass) Members of a lifetime of credit monitoring and identity theft protection services provided by an entity other than Defendant;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order Requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other or further relief as the Court may allow.

DEMAND FOR JURY TRIAL

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

Dated: September 11, 2017

Respectfully submitted,

COAST LAW GROUP LLP
By: s/ *Helen I. Zeldes*
Helen I. Zeldes, Esq. (SBN 220051)
E-mail: helen@coastlaw.com

HUSSIN LAW
BY: s/ *Tammy Gruder Hussin*
Tammy Gruder Hussin (SBN 155290)

Counsel for Plaintiffs Christopher Tanks, Brittany Dixon and the Putative Class

JS 44 (Rev. 06/17)

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
- ☒ 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)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	❒ 4
Citizen of Another State	❒ 2	☒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	☒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

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

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
❒ 190 Other Contract	❒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise				❒ 864 SSID Title XVI	☒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
					❒ 893 Environmental Matters
					❒ 895 Freedom of Information Act
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 896 Arbitration
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 950 Constitutionality of State Statutes
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

X am

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 statue.

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.