Gordon M. Fauth, Jr. (SBN 190280)
gfauth@finkelsteinthompson.com
Of Counsel
Rosanne L. Mah (Cal. Bar No. 242628)
rmah@finkelsteinthompson.com
Of Counsel
FINKELSTEIN THOMPSON LLP
100 Pine Street, Suite 1250
San Francisco, California 94111
Direct Telephone: (510) 238-9610
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Attorneys for Individual and Representative
Plaintiff Malcolm B. Feied

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco-Oakland Division

MALCOLM B. FEIED, an Individual, on behalf of himself and all others similarly situated, Plaintiff, vs. EQUIFAX, INC., a Corporation, Defendant.	Case No. **CLASS ACTION COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF** **JURY TRIAL DEMANDED**

Plaintiff Malcolm B. Feied, individually and on behalf of all others similarly situated, by and through his undersigned counsel, for his complaint brings this class action for damages and equitable relief against Defendant Equifax, Inc. Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge:

NATURE OF THE ACTION

1. This is a civil action brought by Plaintiff Malcolm B. Feied ("Feied" or "Plaintiff") on behalf of himself and all others similarly situated against Defendant Equifax, Inc. ("Equifax" or "Defendant").

2. Equifax is one of the largest consumer credit reporting agencies in the United States and the world. As such, Equifax receives, collects and maintains sensitive personal information belonging to and concerning hundreds of millions of consumers, which it keeps in its computer databases.

3. On or about September 7, 2017, Equifax announced that it had experienced a massive data breach affecting some 143 million consumers in the United States, some 15 million of them California citizens (hereafter, "data breach"). Equifax stated the breach happened because of a vulnerability in one of its website applications. Because of the data breach, which Equifax says occurred from May through July 2017, Plaintiff's and consumers' personal information, including names, addresses, telephone numbers, social security numbers, drivers' license numbers, credit card numbers and other information is now in the hands of unknown hackers and may be used for identity theft and other injurious purposes.

4. Plaintiff and consumers in California and across the United States have suffered harm because of Defendant's failure to take adequate security measures to protect their data and failure to prevent hackers from gaining access to such sensitive information, Defendant's failure to disclose to Plaintiff and others that it did not adequately protect information entrusted to it or over which it has control, and failure to disclose the occurrence of the breach until months after it occurred. The situation is made the more egregious by the fact that Equifax has suffered serious data breaches in the past and was on notice of the need to take effective measures to prevent such a breach. Equifax willfully chose not to take the measures that it knew were necessary to protect the sensitive data in its keeping, and the direct result is the largest consumer data breach of its kind in history, given the scale and the scope of the personal information taken.

5. Defendant's actions and omissions violate laws including the Fair Credit Reporting Act, 15 U.S.C. § 1681 et *seq.*, the Security Breach Notification Law, Cal. Civil Code § 1798.82; the Customer Records Act, Cal. Civ. Code § 1798.81.5; the Unfair Competition Law,

Cal. Bus. and Prof. Code §§ 17200, *et seq.*; and constitute negligence.

6. Accordingly, Plaintiff brings this case as a class action and, on behalf of himself and other similarly situated persons, seeks damages including compensatory damages, statutory and punitive damages, injunctive and equitable relief, declaratory relief, and attorney fees and costs.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because a claim under federal law is pleaded, and pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interests and costs; the number of members of each of the proposed Classes exceeds 100; and Plaintiff and many members of the proposed Plaintiff Classes are citizens of different states than the Defendant.

8. This Court has personal jurisdiction over the Defendant as it conducts substantial business in the State of California and in this Judicial District and/or the conduct complained of occurred in and/or emanated from this State and Judicial District.

9. Venue is proper in this Judicial District because Defendant conducts substantial business in this Judicial District, Plaintiff is a resident of the Judicial District, and/or the conduct complained of occurred in or emanated from this District.

INTRADISTRICT ASSIGNMENT

10. Venue is proper in this Judicial District and the Oakland/San Francisco division thereof pursuant to 28 U.S.C. section 1391 subsections (b) and (c), and Civil L.R. 3-2 subsections (c) and (d). Plaintiff resides in Alameda County within such division, and Defendant transacts business in this division and County and/or a substantial part of the events giving rise to the claims at issue in the litigation arose in this division and County.

PARTIES

11. Plaintiff Malcolm B. Feied is and has at all relevant times been a resident of Alameda County, California and of this Judicial District.

12. According to Equifax, Feied's personal data is implicated in the data breach. As a result of the theft of his personal data in the data breach, he is now forced to expend time, effort

and resources in monitoring activities involving his personal finances and use of his identity and personal information.

13. Defendant Equifax, Inc. is a Georgia corporation with headquarters in Atlanta, Georgia. Its main business consists of, for monetary fees, assembling and/or evaluating consumer credit information or other information on consumers for the purposes of furnishing consumer reports to third parties.

14. Equifax was founded in 1899. Operating throughout the world, it compiles and handles sensitive personal information belonging to millions of consumers worldwide. Equifax operates throughout the United States, with extensive operations in California and this Judicial District, including having multiple offices in this Judicial District. Equifax's wholly-owned subsidiary, TrustedID, Inc., which Equifax involved in the aftermath of the data breach in an attempt to control damage and garner more business from the breach, is located in Palo Alto, California.

SUBSTANTIVE ALLEGATIONS COMMON TO ALL CAUSES OF ACTION

Defendant Knew of the Massive Data Breach for At Least Six Weeks, and Possibly Much Longer, But Failed to Notify Affected Consumers or the Public

15. Equifax is the oldest of the three largest providers of consumer credit information in the United States. As Equifax states in its published reports, the company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide. It solicits, receives and/or collects consumer data from a variety of sources, including directly from consumers, from businesses and financial institutions, and from more than 7,100 employers. It employs approximately 9,500 employees worldwide.

16. Equifax maintains sensitive personal and financial information on many millions of consumers in the United States, including Plaintiff and members of the proposed Classes. It maintains their information in electronic databases. It uses such information to provide credit reports and other reports to third parties, for its own profit.

17. On September 7, 2017, Equifax issued a press release announcing that its information security systems had been hacked in a massive data breach, lasting from May through July 2017, exposing approximately 143 million U.S. consumers' sensitive and personal

information. The information taken by unknown hackers includes names, street addresses, birth dates, social security numbers, driver's license numbers, financial information, credit card information and other personal information ("Personal Information"). The data breach exposed the Personal Information of some 15 million consumers in California alone.

18. In terms of size and the scope of the consumer data taken, the Equifax data breach is unparalleled. While a few other data breaches have been larger in sheer size, the Equifax breach is by far the worst to date in terms of harm to consumers, given the detailed personal information it has provided to the cyberthieves. "On a scale of 1 to 10 in terms of risk to consumers, this is a 10," said Avivah Litan, a fraud analyst at Gartner Research.

19. The September 7, 2017 press release was the first notice Plaintiff and other consumers received that their Personal Information was in jeopardy.

20. According to Equifax, the data breach began as early as mid-May 2017. Equifax has confirmed that at that time hackers entered its system through a web-application vulnerability. Equifax says it became aware of the breach on July 29, 2017. However, according to a September 18, 2017 Bloomberg report, Equifax became aware of a serious security breach in March 2017, four months earlier than reported by Equifax. While acknowledging the March 2017 intrusion, Equifax has denied it was part of the later data breach.

21. Even according to its own timeline, Equifax took approximately six weeks to notify the public about the massive data breach. When Equifax finally announced the cybersecurity incident, it directed consumers to visit a Equifax breach notification website, www.equifaxsecurity2017.com to find out if their personal information had been taken.

22. Incredibly, in addition to waiting to notify consumers of the danger to which it had exposed them, Equifax then attempted (and is attempting) to use the data breach as a business opportunity to enroll consumers in a service that will generate more profit for itself and a wholly-owned subsidiary.

23. At the www.equifaxsecurity2017.com website to which Equifax directed consumers, in addition to telling consumers who entered the requested information whether their personal information was implicated in the data theft, Equifax also involved a company call TrustedID in damage control, attempting to induce affected consumers to have TrustedID

monitor credit activities for them. In enticing affected consumers to enroll with TrustedID, it failed to disclose that TrustedID, based in Palo Alto, California, is its wholly-owned subsidiary, or that the terms of the user agreement for the credit monitoring service would require consumers to arbitrate disputes with TrustedID and Equifax and would prevent them from bringing an action in court (Equifax later stated that it would not seek to enforce the arbitration agreement with respect to the data breach).

24. Despite having been aware of the massive data breach since at least July 2017 and possibly as early as March 2017, Equifax has not yet individually notified consumers whose Personal Information has been allowed to fall into the hands of hackers, to provide them the details of the theft of their personal information as required by law.

25. While Equifax was at least weeks and possibly months late in notifying the public of the data breach, and while it still has not proactively provided individual notification to affected consumers, certain of its executives allegedly took steps to protect their own financial interests before the breach was made public.

26. The Department of Justice has reportedly opened a criminal investigation into whether three top Equifax officials violated insider trading laws when they sold company stock before the massive cyber breach was disclosed publicly. According to Bloomberg News, Federal prosecutors are examining nearly $1.8 million in sales of Equifax stock by chief financial officer John Gamble, Joseph Loughran, president of Equifax's information solutions division, and Rodolfo Ploder, president of its workforce solutions unit.

Defendants' Inadequate Security Measures and Willful and Negligent Practices

27. The data breach was a direct result of Equifax's willful failure to employ reasonable security measures to protect consumers' Personal Information from unauthorized access, including implementation of security measures and technological safeguards to prevent this type of attack and maintenance of security protocols to detect and halt the unauthorized accesses.

28. As the oldest of the three largest credit reporting agencies, Equifax knew that it was constantly at risk of cyber attacks aimed at stealing consumers' Personal Information. Yet, in spite of knowing that the Personal Information it had collected from consumers was targeted

by cyber thieves, Equifax failed to implement proper security procedures and protocols that are standard in the industry and which would have prevented the data breach.

29. Equifax was on notice that its existing security measures were inadequate because it had already experienced multiple serious data breaches—all caused by inadequate security procedures and measures—in which consumers' personal information was accessed by unauthorized third parties.

30. In September 2015, Equifax confirmed that hackers had broken into one of its servers and stolen data belonging to 15 million consumers, including names, dates of birth, addresses, Social Security numbers and/or drivers' license numbers, and other sensitive information.

31. In May 2016, Equifax's W-2 Express website suffered an attack that resulted in the theft of 430,000 names, addresses, social security numbers and other personal information of retail firm Kroger. This resulted in a class action which alleged that Equifax had "willfully ignored known weaknesses in its data security, including prior hacks into its information systems."

32. In spite of these and other previous incidents in which hackers gained access to its system, and in spite of industry warnings that its consumer databases were vulnerable, Equifax willfully chose not to implement security measures to prevent this type of attack. Among other things, Equifax allowed a website application vulnerability to exist--which it says caused the data breach--while easily implemented patches and security measures would have prevented or eliminated that vulnerability. Equifax also chose not to implement security protocols that would have detected the unauthorized accesses and halted or limited the size and scope of the data breach.

33. As a result of its willful, reckless and/or negligent acts and omissions, Equifax has once again exposed personal information of consumers to online hackers--this time in a massive consumer data breach of unprecedented proportions given the size of the breach and the scope of the personal information taken.

Plaintiff and the Class Have Suffered an Injury in Fact That Will Endanger Them For Many Years to Come, if not Forever

34. As a result of the data breach, Plaintiff's and consumers' Personal Information is now in the hands of unknown hackers, and Plaintiff and the Class now face an imminent heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendant's conduct. Accordingly, Plaintiff and the Class have suffered "injury-in-fact." *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C.Cir. 2017).

35. Theft of personal information is a serious and growing problem in the United States. The 2017 Identity Fraud Report by Javelin Strategy & Research reports that, "2016 will be remembered as a banner year for fraudsters as numerous measures of identity fraud reached new heights." According to Javelin, the overall identity fraud incidence rose 16% to affect 6.15% of U.S. consumers—the highest on record--with 15.4 million U.S. identity theft victims, who lost a total of $16 billion.

36. Identity theft is a growth industry. As tracked by the Consumer Sentinel Network, maintained by the Federal Trade Commission, of the 3.1 million consumer fraud complaints filed with law enforcement and private agencies in 2015, 16 percent related to identity theft, with identity theft complaints increasing by more than 47 per cent from 2014.

37. According to a Javelin study, there is a high correlation between having information taken in a data breach and becoming an identity theft victim, with nearly 1 in 4 data breach letter recipients becoming an actual victim of identity fraud. Breaches involving theft of Social Security numbers were found to be the most dangerous.

38. The personal information Equifax allowed hackers to take is particularly dangerous in the hands of ID thieves. That is because it includes sensitive personal information, such as names and addresses, Social Security numbers, birth dates, credit card numbers, driver's license numbers, and other identity information that can be used for identity theft and fraud but which cannot be easily changed or cancelled by Plaintiff and other consumers. In fact, the combination of information stolen in the data breach would be fully sufficient to misappropriate a person's identity for the purpose of opening new accounts, obtaining loans, incurring charges, or engaging in various other financial frauds.

39. Plaintiff and other affected consumers are at much greater risk as a result of the Equifax data breach than if only their credit card information or bank account information had been stolen. Bad as that kind of theft can be, credit cards and bank accounts can be frozen or cancelled quickly and new numbers issued, and that can be accomplished as easily as by making a telephone call to the financial institution. Here by contrast, the Personal Information stolen includes personal identity information that either cannot be changed at all, or only with great difficulty and delay. As a result, Plaintiff and Class members will be forced to live under the threat of ID theft and fraudulent use of their personal data for years to come, and face protracted battles in protecting their good names and financial integrity against the misuse of their Personal Information that is now in the hands of fraud artists and identify thieves.

40. As reported by USA Today, the data breach will endanger and haunt Plaintiff and Class members for many years to come and possibly forever:

> Once hackers gain access to these key pieces of personal data -- which is akin to the DNA of a person's online digital self -- it is at the cyber thieves' disposal forever to cause harm.
>
> "It's very problematic for hackers to have all that important information all in one place," says John Ulzheimer, a credit expert who once worked for Equifax and credit-score firm FICO. "This information is perpetually valuable. You are not going to change your name or date of birth or Social Security number. In five years they will be the same, unlike a credit card that takes five minutes to cancel over the phone."
>
> . . .
>
> The bad news is "this data will be used for years," says Avivah Litan, a security analyst at Gartner. "So, as a consumer, you need to be hyper-vigilant."

-- "Equifax Data Breach Could Create Lifelong Identity Theft Threat," USA Today (Sept. 9, 2017), *found at* https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/.

41. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves can use stolen personal information such as social security numbers to open financial accounts, receive government benefits and incur charges and credit in the victim's name. See http:///www.gao.gov/new.items/d07737.pdf. As the GAO Report states, this type of identity theft is the most harmful because it may take

considerable time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records…[and their] good name."

42. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and money repairing the impact to their good name and credit record. Identity thieves use stolen personal information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, tax fraud, and bank/finance fraud. *See* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

43. It can be expensive for consumers to rectify identify theft. A recent report sponsored by Experian states that the "average total cost to resolve an identity theft-related incident … came to about $20,000." Forty percent of consumers said they were never able fully to resolve their identity theft.

44. Identity theft crimes often involve more than financial loss, causing harm such as loss of reputation, adverse credit reports, and even criminal records. Identity thieves can use the victim's identity to obtain a driver's license or other licenses; commit fraud and other crimes exposing the victim to arrest; and create adverse employment, house rental and other history for the victim.

45. It is also a crime that has effects far beyond the date of the theft. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report: "stolen data may be held for up to one year or more before being used to commit identity theft."

46. Identity theft criminals can easily sell or trade the stolen personal information on the cyber black-market. There are web sites where the stolen information is marketed surprisingly freely, according to industry sources. *See* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/. There are also more clandestine web sites, unlisted by search engines and based in foreign countries, and on the so-called "dark web," where blocks of stolen identity information are traded or sold to anonymous buyers. Often the transactions are in bitcoin or utilize other untraceable methods of

payment.

47. Equifax was targeted for the data theft precisely because the Personal Information it stores is so sensitive and comprehensive as to be valuable for the purpose of identity theft. Thus, there is a heightened and substantial risk the information has already been, or will be, sold and used for identity theft purposes.

48. The injury to Plaintiff and the Classes is fairly traceable to Equifax, because Equifax failed properly to secure their data, subjecting them to the substantial risk of identity theft.

49. For all of the above reasons, Plaintiff and the Classes have suffered harm; and there is a substantial risk of injury to Plaintiff and the Class that is imminent and concrete and that will continue for years to come.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action on behalf of himself and on behalf of two classes--a National Class and a California Class (together "Classes").[1]

51. The National Class is initially defined as follows:

"All persons in the United States whose Personal Information was exposed due to the cyber attack disclosed by Equifax on or about September 7, 2017."

Excluded from the National Class are Defendant, its corporate parents, subsidiaries, officers, directors, employees, and partners.

52. The California Class is initially defined as follows:

"All persons who reside in California whose Personal Information was exposed due to the cyber attack disclosed by Equifax on or about September 7, 2017."

Excluded from the California Class are Defendant, its corporate parents, subsidiaries, officers, directors, employees, and partners.

53. This action has been properly brought and may properly be maintained as a class

[1] If not otherwise clear from the context, "Class" not preceded by "National" or "California" means and includes both the National and California Classes.

action under Rule 23(a)(1-4), Rule 23(b)(1), (2) or (3), and/or Rule 23(c)(4) of the Federal Rules of Civil Procedure and case law thereunder.

Numerosity of the Classes

(Fed. R. Civ. P. 23(a)(1))

54. Members of each Class are so numerous that their individual joinder is impractical. The Classes comprise, at the least, millions of consumers. Approximately 143 million consumers nationwide, including some 15 million consumers in California, had their Personal Information exposed in the data breach. The precise number of the members of each Class, and their addresses, are unknown to Plaintiff at this time, but can be ascertained from Defendant's records. Members of the Classes may be notified of the pendency of this action by mail or email, supplemented (if deemed necessary or appropriate by the Court) by published notice.

Predominance of Common Questions of Fact and Law

(Fed. R. Civ. P. 23(a)(2); 23(b)(3))

55. Common questions of law and fact exist as to all members of the Classes. These questions predominate over the questions affecting only individual members of the Classes. The common legal and factual questions include, without limitation:

(a) Whether Defendant represented that consumers' personal information in its custody was secure when in fact it was not;

(b) Whether Defendant failed to disclose that personal information entrusted to it was at risk of theft owing to Defendant's inadequate security procedures;

(c) Whether, Defendant failed to maintain reasonable procedures designed to limit the furnishing of consumer reports, including the Personal Information, to only those purposes listed in 15 U.S.C. § 1681b;

(d) Whether Defendant failed to implement and maintain reasonable security measures and procedures, appropriate to the information in its custody, to safeguard Class members' personal information, in violation of California Civil Code section 1798.81.5(b);

(e) Whether Defendant was negligent in its handling and protection of Class members' personal information;

(f) When Defendant became aware of the data breach;

(g) Whether Defendant notified Class members of the data breach without unreasonable delay as required by California Civil Code section 1798.82;

(h) Whether Defendant's practices, actions and omissions constitute unlawful, fraudulent and/or unfair business practices in violation of California Business and Professions Code section 17200 *et seq.*;

(i) Whether Defendant was negligent with respect to the safekeeping of the Personal Information in its databases; and

(j) The nature of the relief, including damages and equitable relief, to which Plaintiff and members of the Classes are entitled.

Typicality of Claims

(Fed. R. Civ. P. 23(a)(3))

56. Plaintiff's claims are typical of the claims of the Classes because Plaintiff, like all other Class members, had his personal information in Defendant's custody exposed in the security breach.

Adequacy of Representation

(Fed. R. Civ. P. 23(a)(4))

57. Plaintiff is an adequate representative of the Classes, because his interests do not conflict with the interests of the members of the Classes and he has retained counsel competent and experienced in complex class action and consumer litigation.

58. The interests of the members of the Classes will be fairly and adequately protected by Plaintiff and his counsel.

Superiority of a Class Action

(Fed. R. Civ. P. 23(b)(3))

59. A class action is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and members of the Classes. The damages suffered by each individual members of the Classes, while significant, are small given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. Further, it would be virtually impossible for the members of the Classes

individually to redress effectively the wrongs done to them. And, even if members of the Classes themselves could afford such individual litigation; the court system could not, given the thousands or even millions of cases that would need to be filed. Individualized litigation would also present a potential for inconsistent or contradictory judgments. Individualized litigation would increase the delay and expense to all parties and the court system, given the complex legal and factual issues involved. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief

(Fed. R. Civ. P. 23(b)(1) And (2))

60. In the alternative, this action may properly be maintained as a class action with respect to each Class, because:

(a) the prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudication with respect to individual Class members, which would establish incompatible standards of conduct for the Defendant; or

(b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to individual members of the Classes which would, as a practical matter, be dispositive of the interests of other members of the Classes not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

61. (c) Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive or corresponding declaratory relief with respect to each Class as a whole.

Issue Certification

(Fed. R. Civ. P. 23(c)(4))

62. In the alternative, common questions of fact and law, including those set forth in Paragraph 55 above, are appropriate for issue certification.

FIRST CAUSE OF ACTION

(Willful Violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681)

63. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all members of the National Class.

64. By the acts and omissions set forth herein, Defendant has willfully violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 et *seq.* ("FCRA").

65. Plaintiff and members of the National Class are consumers within the meaning of the FCRA, 15 U.S.C. § 1681a(c).

66. Defendant Equifax is a consumer reporting agency within the meaning of the FCRA, 15 U.S.C. § 1681a(f), because, among other things, it regularly engages in the practice, for monetary fees, of assembling and/or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

67. Plaintiff's and Class members' Personal Information is protected by the FCRA. The Personal Information is a consumer report within the meaning of the FCRA, 15 U.S.C. § 1681a(f).

68. The FCRA required Equifax to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under the FCRA, 15 U.S.C. § 1681b. None of the listed purposes includes furnishing consumer reports to unknown and unauthorized persons or entities such as the hackers who acquired the Personal Information in the data breach.

69. Equifax willfully failed to maintain reasonable procedures designed to limit furnishing of the Personal Information of Plaintiff and Class members to the purposes authorized under the FCRA.

70. Equifax violated the FCRA by furnishing consumer reports to hackers in the data breach and/or by willfully or recklessly allowing unauthorized entities to access Plaintiff's and National Class members' Protected Information.

71. Plaintiff and National Class members have been damaged by Equifax's willful and/or reckless violations of the FCRA.

72. Pursuant to 15 U.S.C. § 1681n(a)(1)(A), Plaintiff and National Class members are each entitled to their actual damages or statutory damages of not less than $100 or greater than $1,000.

73. Pursuant to 15 U.S.C. § 1681n(a)(2), Plaintiff and National Class members are entitled to punitive damages and to their attorney fees and costs of suit.

74. Pursuant to 15 U.S.C. § 1681n(a)(3), Plaintiff and National Class members are entitled to their attorney fees and costs of suit.

SECOND CAUSE OF ACTION

(Negligent Violation of the Fair Credit Reporting Act)

75. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all National Class members

76. By the acts and omissions set forth herein, Defendant has negligently violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 et *seq.* ("FCRA").

77. As set forth above, Plaintiff and National Class members are consumers and Defendant Equifax is a consumer reporting agency within the meaning of the FCRA.

78. Under the FCRA, 15 U.S.C. § 1681b, Equifax was required to maintain reasonable procedures designed to limit the furnishing of consumer reports, including the Personal Information, to the purposes listed therein, none of which allow furnishing consumer reports to unknown and unauthorized persons or entities.

79. Equifax failed to maintain reasonable procedures designed to limit furnishing of the Personal Information of Plaintiff and National Class members to the purposes authorized under the FCRA.

80. As a direct and proximate result of Defendant's negligence, unauthorized persons gained access to and acquired Plaintiff's and National Class members' Protected Information.

81. Plaintiff and Class members have been damaged by Equifax's negligent violations of the FCRA.

82. Accordingly, Plaintiff and National Class members are entitled to their actual damages, and are entitled to their attorney fees and costs of suit.

THIRD CAUSE OF ACTION

(Violation of the Security Breach Notification Law, Cal. Civil Code § 1798.82)

83. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all California Class members.

84. Defendant's acts and omissions violate the Security Breach Notification Law, Cal. Civil Code § 1798.82 et *seq.*

85. Defendant conducts business in California and owns or licenses digital data including, within the meaning of Cal. Civ. Code § 1798.82(h), the Personal Information of California residents, including Plaintiff.

86. Defendant's information security systems were breached, resulting in the theft of California Class members' Personal Information. Defendant learned of the breach no later than July 2017, and possibly months earlier, but has failed to send Plaintiff and individual California Class members timely written notice as required by Cal. Civ. Code § 1798.82, and has failed to provide the information required by law.

87. By failing to timely disclose to Plaintiff and each member of the proposed California Class in the most expedient manner possible that their Personal Information has been acquired by an unauthorized person, Defendant violated Cal. Civ. Code § 1798.82.

88. There was no lawful reason for the delay in notifying Plaintiff and California Class members of the data breach and providing the information required by Cal. Civ. Code § 1798.82.

89. As a direct and proximate result of Defendant's violations of Cal. Civ. Code § 1798.82, Plaintiff and California Class members have suffered harm and damages.

90. Plaintiff and California Class members are therefore entitled to damages, injunctive relief, and attorneys' fees and costs as prayed for hereunder.

//

//

//

//

FOURTH CAUSE OF ACTION

(Violation of the Customer Records Act, Cal. Civ. Code § 1798.80)

91. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. This claim is brought by Plaintiff on behalf of himself and all California Class members.

92. Defendant's acts and omissions violate the California Customer Records Act, Cal. Civ. Code § 1798.80 et *seq.*

93. Equifax is a business that owns or licenses personal information about California residents within the meaning of Cal. Civ. Code § 1798.81.5.

94. By failing to implement and maintain appropriate and reasonable security procedures and practices to protect the Personal Information of Plaintiff and the California Class from unauthorized access and disclosure, Equifax violated Cal. Civ. Code § 1798.81.5.

95. As a result of Equifax's violation of Cal. Civ. Code § 1798.81.5, Plaintiff and California Class members have been injured.

96. Plaintiff and California Class members are therefore entitled to damages, injunctive relief, and reasonable attorneys' fees and costs pursuant to § 1798.84, as prayed for hereunder.

FIFTH CAUSE OF ACTION

(For Negligence and Negligent Failure to Warn)

97. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of both Classes.

98. The actions of Defendant constitute negligence and/or negligent failure to warn.

99. Defendant owed a duty of care to Plaintiff and members of the Classes. Defendant breached that duty.

100. Among other things, Defendant failed to warn Plaintiff and members of the Classes that their Personal Information entrusted to Defendant was not properly protected and that Defendant did not maintain the security procedures and measures reasonable necessary to protect such data from exposure and theft.

101. Among other things, Defendant failed to implement and maintain the security procedures and measures reasonable necessary to protect Plaintiff's and Class members' Personal Information from exposure and theft.

102. Among other things, Defendant failed to notify Plaintiff and members of the Classes in a timely manner of the data breach and of the danger to them caused by the data breach.

103. Among other things, Defendant failed to implement and maintain the security procedures and protocols reasonable necessary to protect Plaintiff's and Class members' Personal Information from exposure and theft.

104. As a direct and proximate result of the practices, acts and omissions alleged herein, Plaintiff and members of the Classes have suffered injury and damages.

105. At all relevant times, Plaintiff and members of the Classes acted lawfully and with due care and did not contribute to the injuries suffered.

106. Because of the harm directly and proximately caused by the breaches of duty and/or acts and omissions described herein, Plaintiff and members of the Classes are entitled to damages and other appropriate relief, as prayed for hereunder.

SIXTH CAUSE OF ACTION

(Violations of the Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq*.)

107. Plaintiff realleges, as if fully set forth, each and every allegation set forth above, and pleads this cause of action on behalf of himself and all members of the California Class.

108. Defendant's business practices as complained of herein violate the Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200, *et seq.* ("UCL").

109. Defendant's practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate statutory law and the common law.

110. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, they are immoral, unethical, oppressive, unconscionable, unscrupulous or substantially injurious to consumers, and/or any utility of such practices is outweighed by the harm caused consumers.

111. Defendant's actions and practices constitute "fraudulent" business practices in violation of the UCL because, among other things, they have a capacity and tendency to deceive members of the public.

112. As a result of Defendant's wrongful business practices, Plaintiff and California Class members have suffered injury in fact.

113. Defendant's wrongful business practices present an ongoing and continuing threat to the general public.

114. Accordingly, Plaintiff is entitled to and prays for judgment and for equitable relief for himself and California Class members, and, where appropriate, members of the general public; and for attorneys' fees and costs of suit, as set forth hereunder.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Classes pray for relief and judgment against Defendant, as follows:

A. Certifying the Classes pursuant to Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiff as representative of the Classes and designating his counsel as counsel for the Classes;

B. Awarding Plaintiff and the Classes compensatory damages, in an amount exceeding $5,000,000, to be determined by proof;

C. Awarding Plaintiff and the Classes statutory damages;

D. Awarding Plaintiff and the Classes punitive damages;

E. For declaratory and equitable relief, including restitution and disgorgement;

F. For an order enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

G. For injunctive relief requiring Defendant to take steps to repair the injury caused by its wrongful conduct;

H. Awarding Plaintiff and the Classes the costs of prosecuting this action, including expert witness fees;

I. Awarding Plaintiff and the Classes reasonable attorney fees;

J. Awarding pre-judgment and post-judgment interest; and

K. Granting other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Malcolm B. Feied hereby demands trial by jury of all claims so triable.

Respectfully submitted,

Date: September 22, 2017

By: /s/ Gordon M. Fauth, Jr.

Gordon M. Fauth, Jr.
Of Counsel
Rosanne L. Mah
Of Counsel
FINKELSTEIN THOMPSON LLP
100 Pine Street, Suite 1250
San Francisco, California 94111
Direct Telephone: (510) 238-9610
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Attorneys for Individual and Representative Plaintiff Malcolm B. Feied

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

MALCOLM B. FEIED, on behalf of himself and all others similarly situated

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Gordon M. Fauth, Jr. (SBN: 190280); Rosanne L. Mah (SBN: 242628); Finkelstein Thompson LLP, 100 Pine St., Ste. 1250, SF CA 94111; Direct Tel. No. (510) 238-9610

DEFENDANTS

Equifax, Inc.

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

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

Attorneys *(If Known)*

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

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

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

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent–Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
15 U.S.C. SECTION 1681 and/or 28 U.S.C SECTION 1332(d)

Brief description of cause:
violations of Fair Credit Reporting Act and consumer protection statutes arising from data breach exposing personal information

VII. REQUESTED IN COMPLAINT:

✔ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

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

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

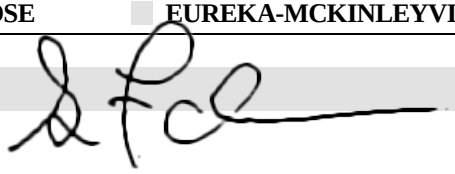
JUDGE Haywood S. Gilliam, Jr. DOCKET NUMBER 4:17-cv-05262

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

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

DATE 09/22/2017

SIGNATURE OF ATTORNEY OF RECORD



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

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

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

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