DEREK G. HOWARD (SBN 118082)
(Derek@derekhowardlaw.com)
ASHLEY M. ROMERO (SBN 286251)
(ashley@derekhowardlaw.com)
DEREK G. HOWARD LAW FIRM, INC.
42 Miller Avenue
Mill Valley, CA 94941
Telephone: (415) 432-7192
Facsimile: (415) 524-2419

DANIEL J. MULLIGAN (SBN 103129)
(dan@jmglawoffices.com)
JENKINS MULLIGAN & GABRIEL LLP
10085 Carroll Canyon Road, Ste. 210
San Diego, CA 92131
Telephone: (858) 527-1792

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL IRWIN, Individually and on behalf of all other similarly situated California citizens,

Plaintiffs,

v.

EQUIFAX INC., a Georgia Corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE;**
2. **VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, *et seq.*;**
3. **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW; and**
4. **UNJUST ENRICHMENT.**

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY OF ALLEGATIONS

1. This case arises from what is now being called the most pervasive data breach in history.

2. Defendant EQUIFAX, INC. is one of three major consumer credit reporting agencies in the United States.

3. Equifax has admitted that it was "hacked,"[1] and personal data about millions of consumers was stolen as a result of Equifax's conduct (the "Breach").

4. In an October 3, 2017 update by Equifax Inc. ("Equifax"), it admitted that the criminals behind the Breach have obtained personal information[2] from at least 145.5 million Equifax user accounts.

5. Plaintiff Michael Irwin's ("Plaintiff") personal information was stolen due to Equifax's failure to create and implement the proper security mechanisms to safeguard Equifax customers' personal information.

6. Plaintiff alleges that Equifax has compromised approximately 17 million California citizens' information.

7. Plaintiff brings this action both individually and on behalf of a defined Class of California citizen, set forth herein.

8. On October 3, 2017, then Equifax CEO William Smith provided testimony to the House of Representatives ("the Testimony") admitting that at a minimum Equifax was negligent, causing the well-publicized Breach to the damage of the alleged class.

9. The Breach occurred during mid-May through July 2017.

10. Equifax claims to have discovered the Breach on July 29, 2017.

11. Equifax waited more than a month from the end of the security breach to advise affected users that their private, personal information had been compromised.

---

[1] The term "hacked" means herein, to circumvent security and break into (i.e. a network, computer, file etc., with malicious intent.

[2] Personal information means information that is personally identifiable, including names, addresses, email addresses, phone numbers and social security numbers and that is not otherwise readily available publicly.

12. On September 7, 2017, Equifax disclosed for the first time that a website application vulnerability allowed the unidentified hackers to breach past and current users' personal information, including Social Security numbers, addresses, and other personal protected information.

13. In addition to the loss of private personal information, the hackers obtained credit card numbers for over 200,000 users, as well as personal identifying information for approximately 180,000 U.S. users related to disputes. The Breach was Equifax's third known major cybersecurity attack since 2015.

14. Despite many industry-wide warnings that Equifax must take active steps to improve its cyber security and data breach detection protocol, Equifax failed on multiple fronts to properly secure the personal information of its users.

15. Equifax failed to create and implement proper security protocols to prevent and detect unauthorized breaches of its information security systems.

16. As one member of Congress stated at the Hearing, the occurrence of the Breach was like leaving Fort Knox unlocked. In other words, Equifax failed to implement basic, standard technology safeguards for very important information.

17. As a direct result of Equifax's failure to adhere to basic cybersecurity, Plaintiff, individually and on behalf of the Class of California citizens, has been damaged. This class action lawsuit follows.

II. JURISDICTION AND VENUE

18. This Court has jurisdiction under 28 U.S.C. § 1332(d) because: (a) this matter was brought as a class action under Fed. R. Civ. P. 23; (b) the class (as defined below) has more than 100 members; (c) the amount at issue exceeds $5,000,000, exclusive of interest and costs; and (d) at least one proposed Class member is a citizen of a state different from Equifax.

19. This Court has personal jurisdiction over Equifax because Equifax transacts substantial business in this judicial district.

20. Venue is proper in this Court under 28 U.S.C. § 1391 because, *inter alia*, Equifax regularly conducts substantial business in this district and is therefore subject to personal

jurisdiction, and because a substantial part of the events giving rise to the Complaint arose in this district

21. This action is not subject to arbitration. Although Equifax's Product Agreement and Terms of Use, last revised September 12, 2017 ("Product Agreement"), contain an arbitration agreement, the Product Agreement carves out actions related to the Breach: "THIS AGREEMENT ALSO DOES NOT APPLY TO THE TRUSTEDID PREMIER PRODUCT OR THE EQUIFAX CYBERSECURITY INCIDENT ANNOUNCED ON SEPTEMBER 7, 2017." *Terms of Use*, Equifax (last visited Sep. 29, 2017), http://www.equifax.com/terms/.

III. INTRADISTRICT ASSIGNMENT

22. Assignment to the San Francisco Division is appropriate under Local Civil Rule 3-2 because the actions that gave rise to the claims in this Complaint arose, in large part, in San Francisco County.

23. Current filings have been assigned to the Hon. Beth Lampson Freeman. This case is related to those earlier filings under the Local Rules of the Northern District of California.

IV. PARTIES

24. Plaintiff Michael Irwin is a natural person, California citizen, and resident of Westminster, California.

25. Plaintiff Irwin is one of the approximately 143 million Equifax whose personal information was compromised because Equifax did not take reasonable steps to secure such information.

26. Defendant Equifax, Inc. is a Georgia incorporated company headquartered at 1550 Peach Street, N.W., Atlanta, Georgia. Equifax is a member of the S&P 500®, and its common stock trades on the New York Stock Exchange under the symbol EFX.

V. FACTUAL BACKGROUND

A. EQUIFAX IS IN THE BUSINESS OF COLLECTING CONSUMERS' PRIVATE INFORMATION

27. Equifax's website reveals how problematic the Breach is when the Company's business is collecting users' private information: "Your credit history is a lot like a fingerprint:

Everyone's credit history is unique, and no one's looks exactly the same."

28. Equifax compiles data about consumers to enable it to provide thorough credit reports to its customers.

29. The credit reports Equifax produces are used by a panoply of financial companies, including mortgage lenders, banks, credit card companies, and retailers.

30. Equifax is one of three major credit bureaus in the United States used by such financial companies.

31. Equifax compiles all possible data about a particular consumer to provide a thorough credit report about the individual.

32. Equifax also provides data analysis so users or lenders can investigate a particular user's credit and financial history.

B. EQUIFAX MAINTAINED A POROUS CYBERSECURITY INFRASTRUCTURE AND INSUFFICENT INVESTIGATIVE REMEDIAL MEASURES

33. The hackers gained access to certain files in the company's system by exploiting a weak point in the website software.

34. Even at the Hearing, Equifax has provided only a vague description of how the Breach occurred, blaming "criminals" who "exploited a U.S. website application vulnerability."

35. However, as additional information develops, it is increasingly apparent that Equifax is deflecting attention from how Equifax's own reckless conduct allowed the Breach.

36. Plaintiff alleges that the Breach over the summer of 2017 occurred due to a known, and fixable, vulnerability in Equifax's web server software.

37. Equifax uses Apache Struts software.[3] Apache Struts is a free, open-source MVC (model-view-controller) framework for creating Java web applications.[4]

38. In early March 2017, security researchers publicly disclosed a bug in the Apache Struts software. This vulnerability could have been patched by Equifax but it was not.

[3] Anna Maria Andriotis, Robert McMillan, and Christina Rexrode, "Equifax Comes Under Attack For Data Breach," *The Wall Street Journal* (Sept. 9-10) at B1-B2.

[4] Apache Struts website, https://struts.apache.org/ (last visited Sep. 29, 2017).

39. This failure to act allowed hackers to access and insert commands into web servers using the Apache Struts software.[5]

40. On or about March 9, 2017, the Apache Software Foundation ("Apache Foundation") issued Security Bulletin S2-045 titled "Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser" (the "Bulletin").

41. The Bulletin announced a "Critical" categorization for the vulnerability, which is the highest security rating issued by the Apache Foundation.

42. Software affected by this critical vulnerability included Struts versions 2.3.5 through 2.3.31 and versions 2.5 through 2.5.10, used by Equifax.

43. The Apache Foundation indicated the problem could be fixed with an "upgrade to Struts 2.3.32 or Struts 2.5.10.1," which could be completed by following easy-to-access, detailed instructions provided free of charge by the Apache Foundation at https://struts.apache.org/docs/s2-045.html.

44. On September 9, 2017, the Apache Foundation released a statement containing comments from the Apache Struts Project Management Committee on the Equifax breach, which, among other things, set out the Apache Foundation's general advice to all Apache Struts users, including Equifax.

45. René Gielen, Vice President of Apache Struts, stated that "[m]ost breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years," and following the Apache Foundation's advice "help[s] to prevent breaches such as unfortunately experienced by Equifax."[6]

46. Rather than immediately taking steps to protect against the vulnerability, it appears that Equifax continued to operate without updating to the latest version of the Apache Struts software. Equifax's decision not to immediately address the known and highly publicized

[5] Dan Goodin, *Critical vulnerability under "massive" attack imperils high-impact sites*," Ars Technical (Mar. 9, 2017 1:07 PM), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/.

[6] *Apache Strust Statement on Equifax Security Breach*, The Apache Software Foundation Blog (Sep. 9, 2017, 3:30 pm), https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax.

vulnerability irresponsibly left open a back door for hackers to steal users' confidential information.

47. The hackers gained access to certain files in Equifax's system from mid-May to July and exploited a weak point in the website software for Equifax's servers.

48. In addition to social security numbers and driver's license numbers, other information compromised included names, date of birth and addresses. Credit card numbers for over 200,000 consumers were stolen, while documents with personal information used in disputes for over 180,000 people were also taken.

49. The severity of the Breach is potentially worse than any in history because the hackers were able to siphon much more personal information than just names and addresses — they stole the keys that unlock consumers' medical histories, bank accounts and employee accounts.

50. Because Social Security numbers do not change, the opportunity for criminals to use the information to the damage of the class cannot be "undone" by closing an account or the like, leaving the Plaintiff and the class vulnerable essentially in perpetuity.

51. Cybersecurity professionals previously criticized Equifax for not improving its security practices.

52. In 2016, identity thieves successfully made off with critical W-2 tax and salary data from an Equifax website.

53. Earlier in 2017, hackers again stole W-2 tax data from an Equifax subsidiary, TALX, which provides online payroll, tax and human resources services to some of the nation's largest corporations.

54. Equifax also houses much of the data that is supposed to be a backstop against security breaches.

55. The also company offers a service that provides companies with the questions and answers needed for their account recovery in the event customers lose access to their accounts.

56. Equifax's Privacy Policy affirmatively represents that it is "committed to protecting the security of [users'] information through procedures and technology designed for

this purpose," and promises that "Before we provide [users] access to [their] credit file disclosure, we verify [their] identity."

57. Notwithstanding Equifax's efforts to spin the damage to the public, it has in reality implemented ineffective cybersecurity measures and demonstrated an inability to take affirmative and necessary investigative and remedial action when the Breach was brought to its attention.

58. In a September 10, 2017 press release, California Attorney General Xavier Bacerra issued a statement confirming that "Millions of Californians' personal information has been compromised as a result of this massive data breach. Equifax's response to date is unacceptable."

59. As noted, Equifax has previously acknowledged the Breach occurred on May 13 and publicly claims that it first discovered the problem on July 29, 2017.

60. Equifax notified the public of the Breach on September 7, 2017. During the Testimony, former CEO Smith added that he first heard about "suspicious activity" in a customer-dispute portal, where Equifax tracks customer complaints and efforts to correct mistakes in their credit reports.

61. CEO Smith and the Equifax Board of Directors moved to hire cybersecurity experts from the law firm King & Spalding to start investigating the Breach on August 2, 2017.

62. However, CEO Smith claimed that, at that time, there was no indication that any customer's personally identifying information had been compromised.

63. As it turns out, after repeated questions from lawmakers during the Testimony, Smith admitted he never asked at the time whether the disclosure of personal protected information was even a possibility.

64. In the Testimony Smith also stated that he didn't ask for a briefing about the "suspicious activity" until August 15, almost two weeks after the special investigation began and 18 days after the initial red flag.

65. CEO Smith received the briefing from King & Spalding and other forensic investigators on August 17, 2017.

66. At that point, he said, those monitoring the situation had a better sense of the situation's severity. But CEO Smith still staunchly maintains that he didn't have full information on August 17. "I did not know the size, the scope of the breach," he claimed.

67. On August 22, 2017, CEO Smith belatedly notified the presiding director of Equifax's board, while the entire Board of Directors was briefed on August 24 and 25, 2017.

68. In the Testimony, Smith also testified, that "The picture was very fluid ….We were learning new pieces of information each and every day. As soon as we thought we had information that was of value to the board I reached out."

VI. CLASS ACTION ALLEGATIONS

69. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), Plaintiff brings this action individually and on behalf of a class defined as follows: All California citizens whose personal information was compromised by the Breach disclosed by Equifax on September 7, 2017. ("the Class Members").

70. Plaintiff is a member of the proposed Class of California citizens he seeks to represent.

71. This action is brought and may properly be maintained as a class action pursuant to 28 U.S.C. § 1332(d). This action satisfies the procedural requirements set forth in Fed. R. Civ. P. 23.

72. Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members were damaged by the same wrongful practices of Defendant.

73. Plaintiff will fairly and adequately protect and represent the interests of the Class of California citizens. The interests of Plaintiff are coincident with, and not antagonistic to, those of the Class of California citizens.

74. Plaintiff has retained counsel competent and experienced in complex class action litigation.

75. Members of the Class of California citizens are so numerous that joinder is impracticable. Plaintiff believes that there are millions of California citizens in the Class.

76. Questions of law and fact common to the members of the Class predominate over

questions that may affect only individual Class Members, because Defendant has acted on grounds generally applicable to the entire Class. Thus, determining damages with respect to the Class of California citizens as a whole is appropriate.

77. There are substantial questions of law and fact common to the Class consisting of California citizens. The questions include, but are not limited to, the following:

a. Whether Defendant failed to employ reasonable and industry-standard measures to secure and safeguard its users' personal information;

b. Whether Defendant properly implemented and maintained security measures to protect its users' personal information;

c. Whether Defendant's cybersecurity failures harmed the personal information of California citizens whose information was accessed by criminals or third parties who sought to gain financially from its improper use;

d. Whether Defendant negligently failed to properly secure and protect the personal information of California citizens;

e. Whether Plaintiff and other members of the Class of California citizens are entitled to injunctive relief; and

f. Whether Plaintiff and other members of the Class of California citizens are entitled to damages and the measure of such damages.

78. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated individuals to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. Plaintiff knows of no special difficulty maintaining this action that would preclude its maintenance as a class action on behalf of California citizens.

///

///

///

///

COUNT ONE

NEGLIGENCE

(Plaintiff Individually and All Class Members)

79. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

80. Equifax had an affirmative duty to exercise reasonable care in safeguarding and protecting the personal information of its users. By maintaining their personal information in a database that was accessible through the Internet, Equifax owed Plaintiff and Class Members a duty of care to employ reasonable Internet security measures to protect this information.

81. Equifax, with reckless disregard for the safety and security of users' personal information it was entrusted with, breached the duty of care owed to Plaintiff and the Class by failing to implement reasonable security measures to protect its users' sensitive personal information. In failing to employ these basic and well-known Internet security measures, Equifax departed from the reasonable standard of care and violated its duty to protect the personal information of Plaintiff and all Class Members. Equifax further breached its duty of care by allowing the breach to continue undetected and unimpeded for a period of time after the hackers first gained access to Defendant's systems.

82. The unauthorized access to the personal information of Plaintiff and all Class Members was reasonably foreseeable to Equifax.

83. Neither Plaintiff nor other Class Members contributed to the security breach or Equifax's employment of insufficient and below-industry security measures to safeguard personal information.

84. It was foreseeable that Equifax's failure to exercise reasonable care in protecting personal information of its users would result in Plaintiff and the other Class Members suffering damages related to the loss of their personal information.

85. As a direct and proximate result of Equifax's reckless conduct, Plaintiff and Class Members were damaged. Plaintiff and Class members suffered injury through the public disclosure of their personal information, the unauthorized access to accounts containing

additional personal information, and through the heightened risk of unauthorized persons stealing additional personal information. Plaintiff and Class Members have also incurred the cost of taking measures to identify and safeguard accounts put at risk by disclosure of the personal information stolen from Equifax.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

COUNT TWO

VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, *ET SEQ.*

(Plaintiff Individually and All Class Members)

86. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

87. California Civil Code § 1798.80, *et seq*. (the "Customer Records Act") requires any person conducting business in California and owning computerized data to disclose data breaches to affected users if the breach exposed unencrypted personal information.

88. The Customer Records Act also requires that the notice be made in the most expedient time possible without any unreasonable delay.

89. Equifax failed to notify users of the Breach in an expedient fashion.

90. The Breach qualifies as a "breach of security system" of Equifax within the meaning of Civil Code § 1798.82(g).

91. Equifax is liable to Plaintiff and the Class Members for $500.00 pursuant to Civil Code § 1798.84(c), or up to $3,000.00 per class member if Equifax's actions are deemed willful, intentional, and/or reckless.

92. Equifax is also liable for Plaintiff's reasonable attorneys' fees and costs pursuant to Civil Code § 1798.84(g).

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

COUNT THREE

VIOLATION OF CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200, *ET SEQ.*

(Plaintiff individually and All Class Members)

93. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set

forth herein.

94. California's Unfair Competition Law ("UCL") is designed to protect consumers from illegal, fraudulent, and unfair business practices.

95. Equifax's practice of representing that it adequately protected users' financial and personal information, while Equifax in fact employed lax and ineffective security measures in order to cut costs, is a deceptive business practice within the meaning of the UCL.

96. In fact, Equifax continues to employ lax and ineffective security measures as to the non-public, financial and personal information of users.

97. Thus, Equifax continues to engage in deceptive business practices.

98. Equifax's practice of withholding information about the Breach from its users is also a deceptive business practice within the meaning of the UCL, because users reasonably expect to be notified if their non-public, financial and personal information is compromised.

99. Equifax's practices are unfair because they allowed Equifax to profit while simultaneously exposing Equifax users, such as Plaintiff, to harm in the form of an increased risk of having their personal information stolen, which in fact occurred: the Breach.

100. Such harm was not foreseeable, as Plaintiff and the Class expected Equifax to employ industry-standard security measures, including cybersecurity firewalls to prevent a Breach and investigative tools to timely discover one, and to promptly disclose any data breach.

101. Equifax's deceptive business practices induced Plaintiff and the Class to use Equifax's services and provide personal information to Equifax.

102. As a direct result of Equifax's deceptive business practices, Plaintiff and the Class have been and are being damaged.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

COUNT FOUR

UNJUST ENRICHMENT

(Plaintiff individually and All Class Members)

103. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

104. As a result of Equifax's misleading representations and omissions concerning the adequacy of its data security practices, Plaintiff and Class Members were induced to believe that when Equifax maintained and otherwise used their non-public, financial and personal information, there would be no harm or damage to Plaintiff and the Class Members.

105. While operating in a misleading and/or negligent fashion, Equifax has derived substantial revenues due to its use and maintenance of Plaintiff and the Class Members' non-public, financial and personal information.

106. In addition, Equifax saved on the substantial cost of providing adequate data security to Plaintiff and the Class.

107. Equifax's cost savings came at the direct expense of the privacy and confidentiality of the non-public, financial and personal information belonging to Plaintiff and the Class Members.

108. Plaintiff and the Class have been damaged and continue to be damaged by Equifax's actions, and Equifax has been unjustly enriched thereby.

109. Plaintiff and the Class are therefore entitled to damages as a result of Equifax's unjust enrichment, including the disgorgement of all revenue received and costs saved by Equifax as a result of the Breach.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class of California citizens, respectfully requests that the Court:

A. Determine that this action may be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3);

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

C. Appoint Plaintiff as Class Representative;

D. Appoint Plaintiff's counsel as Class Counsel;

E. Enter judgment against Defendant and in favor of Plaintiff and the Class;

F. Adjudge and decree that the acts alleged herein by Plaintiff and the Class against Defendant constitute negligence, violation of California Civil Code § 1798.80, *et seq.*, violation of California's Unfair Competition Law, and unjust enrichment;

G. Award all compensatory and statutory damages to Plaintiff and the Class in an amount to be determined at trial;

H. Award restitution, including the disgorgement of all revenue received and costs saved by Equifax as a result of the Breach, payable to Plaintiff and the Class;

I. Award punitive damages, including treble and/or exemplary damages, in an appropriate amount;

J. Enter an injunction permanently barring continuation of the conduct complained of herein, and mandating that Defendant and any successors in interest, be required to adopt and implement appropriate systems, controls, policies and procedures to protect the non-public, financial and personal information of Plaintiff and the Class;

K. Award Plaintiff and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest; and

L. Grant such other and further relief as is necessary to correct for the effects of Defendant's unlawful conduct and as the Court deems just and proper.

Dated: October 4, 2017

JENKINS MULLIGAN & GABRIEL LLP
DEREK G. HOWARD LAW FIRM, INC.

/s/Derek G. Howard
DEREK G. HOWARD
Attorneys for Plaintiff

JURY DEMAND

Plaintiff respectfully demands trial by jury on all issues so triable.

Dated: October 4, 2017

JENKINS MULLIGAN & GABRIEL LLP
DEREK G. HOWARD LAW FIRM INC.

/s/ Derek G. Howard
DEREK G. HOWARD
Attorneys for Plaintiff