UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CHRISTIAN DUKE and DALE MILLER, Individually, and on Behalf of All Others Similarly Situated, Plaintiffs, v. EQUIFAX INC., a Delaware corporation, Defendant.	Civil Action No. CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

Plaintiffs Christian Duke and Dale Miller (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned attorneys, bring this Class Action Complaint against defendant Equifax Inc. ("Defendant," "Equifax," or the "Company"), on behalf the roughly 143 million consumers across the United States harmed by Equifax's failure to protect their highly sensitive personal information. Plaintiffs make the following allegations, except as to personal allegations pertaining to Plaintiffs, upon information and belief based upon the investigation of counsel and review of public documents.

INTRODUCTION

1. Defendant Equifax is one of the three major credit reporting agencies in the United States. Equifax collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide.

2. As a credit reporting agency, Equifax has some of the most intimate information on hundreds of millions of individuals around the world including their names, social security numbers, birthdays, home addresses, and other personal matters. Equifax does not need the individual's consent to gain access to highly personal information about him or her. Rather, Equifax is given the information on hundreds of millions of people by banks, credit card companies, financial institutions, and other companies. Equifax then compiles the information and then sells the information to credit card firms, banks, marketers, and various other entities.

3. Due to the highly sensitive nature of the information under its control, Equifax has a legal duty to protect and keep private consumers' personal data. Equifax repeatedly assured the public that it was a "trusted steward" of consumers' personal information. Equifax also repeatedly touted the "security of its services" and gave the public the impression that their data was safe.

4. However, Equifax did not take the necessary precautions to safely secure the data of hundreds of millions of people. In fact, Equifax's security

system suffered from multiple security breaches starting in at least 2013. Nevertheless, Equifax chose to ignore the many red flags that indicated its system was susceptible to breach.

5. The worst of these security breaches occurred in May 2017. During that time, hackers were able to access the reams of personal data that Equifax possessed because of vulnerability in the Company's Apache Struts web server software. Equifax was on notice that its Apache Struts software had a critical flaw because hackers exploited the flaw to gain access to the Company's data several months earlier. However, Equifax took no action to patch its systems to prevent another incident.

6. Hackers roamed undetected in Equifax's computer network for several months before the Company noticed the massive security breach. However, even after Equifax eventually discovered the breach on July 29, 2017, it did not inform the public about it until September 7, 2017.

7. Just as troubling, three Equifax executives sold shares of their personally held Equifax stock, almost immediately after Equifax discovered the breach, but before it disclosed it to the public. The sales by the three Company executives totaled over $1.8 million.

8. As a result of Equifax's failure to reasonably and adequately secure its network, the data of over 143 million Americans has been compromised. In

addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers were obtained by the hackers. The Plaintiffs and members of the Class (as defined herein) are now at considerable risk for being victims of fraud, identity theft, and other criminal acts which can greatly deteriorate their credit score and lead them to financial ruin.

9. Plaintiffs, individually and on behalf of all Class members, seek actual damages, equitable relief, injunctive relief, restitution and/or disgorgement, attorneys' fees, litigation expenses, and costs of suit because of Equifax's wrongful business practices.

JURISDICTION AND VENUE

10. This Court has original jurisdiction over all counts asserted herein under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the matter in controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs and more than two-thirds of the Class reside in states other than the states in which Defendant is a citizen and in which this case is filed, and therefore any exemptions to jurisdiction under 28 U.S.C. §1332(d) do not apply.

11. Venue is proper in this Court pursuant to 28 U.S.C. §1391, because Plaintiffs reside and suffered injury as a result of Defendant's acts in this District, many of the acts and transactions giving rise to this action occurred in this District,

Defendant conducts substantial business in this District, Defendant has intentionally availed itself of the laws and markets of this District, and Defendant is subject to personal jurisdiction in this District.

THE PARTIES

12. Plaintiff Christian Duke ("Duke") is, and at all times relevant hereto has been, a citizen of the State of California. Plaintiff Duke is one of the more than 143 million American consumers whose personal information was stolen because Equifax failed to adequately protect his information.

13. Plaintiff Dale Miller ("Miller") is, and at all times relevant hereto has been, a citizen of the State of Texas. Plaintiff Miller is one of the more than 143 million American consumers whose personal information was stolen because Equifax failed to adequately protect his information.

14. Defendant Equifax is a Georgia corporation with principal offices at 1550 Peachtree Street N.W., Atlanta, Georgia. It provides credit information services to millions of businesses, governmental units, and consumers across the globe.

FACTUAL ALLEGATIONS

15. Equifax is the oldest of the three major credit-reporting agencies in the United States. The Company collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide.

16. As a credit reporting agency, Equifax has access and custody to some of the most intimate information on hundreds of millions of individuals including their names, social security numbers, birthdays, home addresses, and other personal information. Equifax also has intimate knowledge of consumers' loans, loan payments, credit cards, child support payments, credit limits, missed rent payments, and employer history. Equifax does not need the consent of consumers to gain access to highly personal information about them. Rather, Equifax is given the information on hundreds of millions of people by banks, credit card companies, financial institutions, and other companies. Equifax then compiles the information into detailed files and sells them back to credit card firms, banks, marketers, and various other entities. Much of this information is used to create credit scores for consumers.

17. Due to the highly sensitive nature of the information under its control, Equifax has a legal duty to protect and keep private the personal data of consumers. As a credit-reporting agency, Equifax is well aware that it sits on a treasure trove of personal information that is worth billions of dollars and is highly coveted by hackers and the innumerable amount of criminals who profit from identification theft.

18. Accordingly, Equifax has repeatedly touted the Company's commitment to security and safeguarding the data of consumers in numerous

public filings and on its own website. For instance Equifax has claimed in its 2015 and 2016 Annual Reports that it "continue[s] to invest in and develop new technology to enhance the functionality, cost-effectiveness and security of [its] services." In those two public filings, Equifax further stated that it "serve[s] as a trusted steward and advocate for [its] customers and consumers." In addition, Equifax claims that its website "is secured with the highest level of SSL Certification encryption." Equifax also states on its website "[w]e know how important it is for our online transactions to be secure. We safeguard the privacy of the information you give us when you fill out our forms online."

19. Unfortunately, the data that Equifax controlled was anything but secure. Since at least 2014, Equifax was on notice that the system in place to protect against identity theft was vulnerable to attack from hackers. For instance, in April 2013, Equifax suffered a security breach that went unimpeded until the Company discovered it in January 2014. Equifax stated that an "IP address operator was able to obtain the credit reports using sufficient personal information to meet Equifax's identity verification process."

20. Equifax had another breach in May 2016, when one of its websites had suffered an attack that resulted in the leak of 430,000 names, addresses, social security numbers, and other personal information of retail firm The Kroger Co. This breach resulted in a lawsuit from Kroger employees alleging that Equifax had

"willfully ignored known weaknesses in its data security, including prior hacks into its information systems." The lawsuit was eventually dropped with prejudice under the stipulation that Equifax had to fix its serious security problems with one of its websites.

21. In addition, Equifax suffered another security breach between April 2016 and March 2017, when hackers accessed tax records through one of the Company's subsidiaries TALX, a payroll and tax service provider.

22. Despite all these incidents, Equifax did not properly address the vulnerabilities of its security system. As a result, Equifax was susceptible to a cybersecurity breach by hackers.

23. The worst of these security breaches occurred around May 2017. During that time, hackers were able to access the reams of personal data that Equifax possessed because of vulnerability in the Company's Apache Struts web server software. Equifax was on notice that its Apache Struts software had a critical flaw because hackers exploited that same vulnerability in the Apache software in the March 2017 breach. Furthermore, security researchers at Cisco Systems Inc. publicly warned of the flaw in Apache Struts on March 10, 2017, and a patch was issued by the Apache Software Foundation to fix it. However, Equifax did not apply the patch.

24. Equifax eventually discovered the security breach on July 29, 2017. However, Equifax said nothing to the public until September 7, 2017, when it revealed that 143 million individuals had their personal data compromised. The delay in the disclosure of the hack made the situation even worse for the affected individuals because it allowed identity thieves extra time to make use of the their personal data. Equifax also revealed that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers were obtained by the hackers.

25. To make matters worse, three Equifax executives sold shares of their personally held Equifax stock after the discovery of the breach but before the Company disclosed it to the public. The sales were made three to four days after the breach was discovered. In particular, on August 1, 2017, Equifax's Chief Financial Officer, John Gamble, sold his shares worth $946,374 and President of U.S. Information Solutions, Joseph Loughran, exercised options to dispose of his stock worth $584,099. The following day, Equifax's President of Workforce Solutions, Rodolfo Ploder, sold $250,458 of his stock. Altogether, the three executives collected $1.8 million from the sales.

26. As a result of Equifax's unlawful, unfair, inadequate, and unreasonable security, cybercriminals now possess the personal data of Plaintiffs

and the other Class members. At least 143 million American consumers stand to become victims of identity theft. Identity thieves will be able to use Plaintiffs and Class members' personal information to take out loans, mortgage property, open financial accounts, sign up for credit cards, obtain government benefits, file fraudulent tax returns, obtain medical services, and provide false information to police during an arrest. Even if Plaintiffs and Class members timely discover that their identity was stolen, they can still suffer considerable damage to their financial position and credit scores that can impact the rest of their lives.

CLASS ACTION ALLEGATIONS

27. Pursuant to Rule 23 of the Federal Rules of Civil Procedure ("Rule 23"), Plaintiffs bring this action as a national class action for themselves and all members of the following class of similarly situated individuals and entities (the "Class"):

> All natural persons and entities in the United States whose personal data Equifax collected and stored and whose personal information was placed at risk or compromised by the data breach that occurred between May and July 2017.

28. In addition, pursuant to Rule 23, Plaintiff Duke brings this action for himself and all members of the following subclass of similarly situated individuals and entities (the "California Subclass"):

> All natural persons and entities residing in California whose personal data Equifax collected and stored and whose personal information was

> placed at risk or compromised by the data breach that occurred between May and July 2017.

29. Moreover, pursuant to Rule 23, Plaintiff Miller brings this action for himself and all members of the following subclass of similarly situated individuals and entities (the "Texas Subclass"):

> All natural persons and entities residing in Texas whose personal data Equifax collected and stored and whose personal information was placed at risk or compromised by the data breach that occurred between May and July 2017.

30. Excluded from the Class is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

31. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleged the same claims.

32. ***Numerosity***. The Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Class members has not been determined at this time, Plaintiffs are informed and believe that millions of persons had their personal data compromised in the data breach that occurred between May and July 2017.

33. ***Commonality***. Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, inter alia:

(a) whether Defendant owed a duty to Plaintiffs and Class members to adequately protect their personal information;

(b) whether Defendant breached its duties to adequately protect the personal information of Plaintiffs and Class members;

(c) whether Defendant knew or should have known that its security system was vulnerable to being hacked;

(d) whether Defendant failed to implement proper safeguards to protect against Plaintiffs' and Class members' information being stolen;

(e) whether Defendant failed to notify consumers of the data breach within a reasonable period of time;

(f) whether Plaintiffs and Class members are entitled to damages, injunctive relief, or other equitable relief; and

(g) the method of calculation and extent of damages for Plaintiffs and Class members.

34. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class members were injured through the uniform misconduct described above and assert the same claims for relief.

35. ***Adequacy***. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs have no interests antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

36. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiffs and the Class members. Plaintiffs and the Class members have been harmed by Equifax's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Equifax's wrongful actions and/or inaction.

37. Class certification, therefore, is appropriate under Rule 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

38. Class certification also is appropriate under Rule 23(b)(2) because Equifax has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

39. The expense and burden of litigation would substantially impair the ability of Plaintiffs and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Equifax will retain the benefits of its wrongdoing despite its serious violations of the law.

COUNT I

(Against Defendant for Negligence on Behalf of Plaintiffs and the Class)

40. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

41. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding their personal information.

42. Defendant owed a duty to Plaintiffs and Class members to implement adequate security checks to timely detect any breaches to the personal data of consumers.

43. Defendant owed a duty to promptly notify Plaintiffs and Class members when their personal information was compromised.

44. Defendant breached its duties by, among other things: (i) failing to implement and maintain adequate data safeguards to protect Class members' personal data; (ii) failing to detect and end the data breach in a timely manner; (iii) failing to disclose that Defendant's data security practices were inadequate and vulnerable to hackers; and (iv) failing to provide adequate and timely notice of the

breach.

45. But for Defendant's breach of its duties, Class members' personal data would not have been accessed by unauthorized individuals.

46. 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 Class members.

47. As a result of Equifax's negligence, Plaintiffs and Class members suffered and will continue to suffer injury, which includes, but is not limited to, inconvenience and 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. Through its failure to timely discover and provide clear notification of the data breach to consumers, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their personal data.

48. The damages to Plaintiffs and Class members were a direct, proximate, reasonably foreseeable result of Defendant's breaches of its duties.

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

COUNT II

(Against Defendant for Negligence Per Se on Behalf of Plaintiffs and the Class)

50. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

51. Because Defendant was aware of a breach of its security system, Equifax had an obligation to disclose it in a timely and accurate fashion. Defendant's failure to maintain adequate security of consumer's personal data and failure to promptly disclose the fact of the breach violates California law, including the California Financial Information Privacy Act, Cal. Fin. Code §4050, *et seq*. and/or the California Customer Records Act, Cal. Civ. Code §1798.80, *et seq*. *See, e.g.*, Cal. Civ. Code §1798.82(a)-(b). Defendant's failure to comply with these applicable laws and regulations constitutes negligence per se.

52. But for Defendant's violation of the applicable laws and regulations, Plaintiffs and Class members' personal data would not have been accessed by unauthorized individuals.

53. As a result of Defendant'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. 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 to deter or detect identity theft.

54. The damages to Plaintiffs and Class members were a proximate, reasonably foreseeable result of Defendant's breaches of the applicable laws and regulations.

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

COUNT III

(Against Defendant for Violations of California Data Breach Notification Law, California Civil Code §1798.80, *et seq*., on Behalf of Plaintiff Duke and the California Subclass)

56. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

57. Pursuant to §1798.82 of the California Civil Code:

> (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information

was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]	Date: [insert date]
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii)

> the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

58. As alleged above, Defendant knew that there was a security breach on July 29, 2017, yet did not tell the public about it until September 7, 2017. The security breach compromised the personal data of 143 million Americans, including Plaintiff Duke and the California Subclass.

59. Defendant failed to disclose to Plaintiff Duke and the California Subclass, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, personal data when it knew or reasonably believed such information had been compromised.

60. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff Duke or the California Subclass would impede its investigation.

61. Pursuant to §1798.84 of the California Civil Code:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> (b) Any customer injured by a violation of this title may institute a civil action to recover damages.
>
> (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.
>
> * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

62. As a result of Defendant's violation of California Civil Code §1798.82, Plaintiff Duke and the California Subclass members' personal data and financial information were compromised, placing them at a greater risk of identity theft, and their private information was disclosed to third parties without their consent. Plaintiff Duke and the California Subclass also suffered diminution in value of their personal data as it is now easily accessible to hackers and criminals who can buy and sell it in the black market. Plaintiff Duke and the California Subclass have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. Plaintiff Duke and the California Subclass are further damaged as their personal data remains in Defendant's

possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

63. Plaintiff Duke, on behalf of himself and members of the California Subclass, seeks all remedies available under California Civil Code §1798.84, including, but not limited to: (i) damages suffered by Plaintiff Duke and the other California Subclass members as alleged above; (ii) statutory penalties of up to $3,000 per violation for Defendant's willful, intentional, and/or reckless violations of California Civil Code §1798.83 (or, at a minimum, up to $500 per violation); and (iii) equitable relief.

63. Plaintiff Duke, on behalf of himself and members of the California Subclass, also seeks reasonable attorneys' fees and costs under California Civil Code §1798.84(g).

COUNT IV

(Against Defendant for Violations of California Unfair Competition Law, California Business & Professions Code §17200, *et seq.*, on Behalf of Plaintiff Duke and the California Subclass)

65. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

66. The Unfair Competition Law prohibits any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code §17200.

Unlawful

67. Defendant engaged in unlawful acts and practices with respect to its services by having inadequate security system to protect consumer's personal information and by soliciting and collecting Plaintiff Duke and the California Subclass members' personal data with knowledge that the information would not be properly protected.

68. In addition, Defendant engaged in unlawful acts and practices with respect to its services by failing to discover and then disclose the data breach to Plaintiff Duke and the California Subclass members in a timely and accurate manner. To date, Equifax has still not provided such sufficient information to Plaintiff Duke and the California Subclass members.

69. As a direct and proximate result of Equifax's unlawful practices and acts, Plaintiff Duke and the California Subclass members were injured and lost money or property including, but not limited to, the price received by Equifax for its services, the loss of their legally protected interest in the confidentiality and privacy of their personal information, and additional losses described above.

70. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Duke and the California Subclass members' highly sensitive information and that the risk of a data breach or theft was very likely.

71. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless.

Unfair

72. Defendant engaged in unfair acts and practices with respect to its services by establishing deficient security system and procedures and by soliciting and collecting Plaintiff Duke and the California Subclass members' personal information with knowledge that the information would not be adequately protected.

73. In addition, Equifax engaged in unfair acts and practices with respect to its services by failing to discover and then disclose the data breach to Plaintiff Duke and the California Subclass members in a timely and accurate manner, and by failing to take proper action following the data breach to implement proper security measures to protect Plaintiff Duke and the California Subclass members' highly sensitive information from further unauthorized disclosure, release, data breaches, and theft.

74. As a direct and proximate result of Defendant's unfair practices and acts, Plaintiff Duke and the California Subclass members were injured and lost money or property including, but not limited to, the price received by Defendant for its services, the loss of their legally protected interest in the confidentiality and

privacy of their personal information, and additional losses described above.

75. Defendant knew or should have known that its security system was inadequate to safeguard Plaintiff Duke and the California Subclass members' personal data and that the risk of a data breach or theft was very likely.

76. Defendant's actions in engaging in the above-named unfair practices and acts were negligent, knowing and willful, and/or wanton and reckless.

77. Plaintiff Duke and the California Subclass members seek relief under California Business & Professions Code §17200, *et seq*., including, but not limited to, restitution of Plaintiff Duke and the California Subclass members' money or property that Defendant may have acquired by means of its unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to Equifax because of its unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT V

(Against Defendant for Violations of the Deceptive Trade Practices Act, Texas Business & Commercial Code §17.46 on Behalf of Plaintiff Miller and the Texas Subclass)

78. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

79. Defendant has violated Texas Business & Commercial Code §17.46, which prohibits false, misleading, or deceptive acts or practices in the conduct of any trade or commerce and any unconscionable action or course of action.

80. Defendant engaged in unfair or deceptive acts or practices by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Miller and the Texas Subclass members' personal data from unauthorized disclosure, release, data breaches, and theft. These representations deceived Plaintiff Miller and the Texas Subclass members into believing their personal data was safe and stored securely.

81. Defendant engaged in unfair or deceptive acts or practices by failing to timely inform Plaintiff Miller and the Texas Subclass members that their personal data was compromised.

82. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the personal data of Plaintiff Miller and the Texas Subclass members and that the risk of a data breach was highly likely and that its failure to notify Plaintiff Miller and the Texas Subclass members of the theft of their data would cause them to sustain further injury.

83. As a direct and proximate result of Equifax's deceptive practices and acts, Plaintiff Miller and the Texas Subclass members who used Equifax's services were injured and lost money or property including, but not limited to, the loss of

their legally protected interest in the confidentiality and privacy of their personal information; damages arising from unauthorized charges on their debit or credit cards that were fraudulently obtained through the use of the personal data of Plaintiff Miller and the Texas Subclass members; and damages from lost time and effort to mitigate the actual and potential impact of the data breach by closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

84. Plaintiff Miller and the Texas Subclass members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages, and attorneys' fees pursuant to the Texas Deceptive Trade Practices Act, costs, and such other further relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for judgment against Defendant as to each and every count, including:

A. An order declaring this action to be a proper class action, appointing Plaintiffs and their counsel to represent the Class, California Subclass, and Texas Subclass, and requiring Defendant to bear the costs of class notice;

B. An order for injunctive relief requiring Defendant to: (i) identify all affected customers; (ii) proactively monitor the personal information of all

potentially affected customers; (iii) engage third-party auditors and internal personnel to conduct testing on Defendant's system on a periodic basis; (iv) strengthen its security system and promptly correct any problems or issues detected; and (v) 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 awarding declaratory relief, and any further retrospective or prospective injunctive relief permitted by law or equity, including enjoining Defendant from continuing the unlawful practices alleged herein, and injunctive relief to remedy Defendant's past conduct;

D. An order requiring Defendant to disgorge or return all monies, revenues, and profits obtained by means of any wrongful or unlawful act or practice;

E. An order requiring Defendant to pay all actual and statutory damages permitted under the counts alleged herein;

F. An order requiring Defendant to pay punitive damages on any count so allowable;

G. An order awarding attorneys' fees and costs to Plaintiffs, the Class, California Subclass, and Texas Subclass; and

H. An order providing for all other such equitable relief as may be just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Respectfully submitted, this 26th day of September, 2017.

ROBBINS GELLER RUDMAN & DOWD LLP

/s/ *John C. Herman*

JOHN C. HERMAN
(Georgia Bar No. 348370)
Monarch Centre, Suite 1650
3424 Peachtree Road, N.E.
Atlanta, GA 30326
Telephone: 404/504-6500
Facsimile: 404/504-6501
jherman@rgrdlaw.com

ROBBINS ARROYO LLP
BRIAN J. ROBBINS (*pro hac vice* to be filed)
KEVIN A. SEELY (*pro hac vice* to be filed)
ASHLEY R. RIFKIN (*pro hac vice* to be filed)
STEVEN M. MCKANY (*pro hac vice* to be filed)
600 B Street, Suite 1900
San Diego, CA 92101
Telephone: 619/525-3990
Facsimile: 619/525-3991
brobbins@robbinsarroyo.com
kseely@robbinsarroyo.com
arifkin@robbinsarroyo.com
smckany@robbinsarroyo.com

ROBBINS GELLER RUDMAN & DOWD LLP
PAUL J. GELLER (*pro hac vice* to be filed)
STUART A. DAVIDSON (*pro hac vice* to be filed)
MARK J. DEARBORN (*pro hac vice* to be filed)
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
Facsimile: 561/750-3364
pgeller@rgrdlaw.com
sdavidson@rgrdlaw.com
mdearborn@rgrdlaw.com

Attorneys for Plaintiffs

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 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 is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

CHRISTIAN DUKE and DALE MILLER, Individually and on Behalf of All Others Similarly Situated

DEFENDANT(S)

EQUIFAX INC., a Delaware corporation

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF California
(EXCEPT IN U.S. PLAINTIFF CASES)

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

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

JOHN C. HERMAN
ROBBINS GELLER RUDMAN & DOWD LLP
3424 Peachtree Road, N.E, Suite 1650
Atlanta, GA 30326
(404) 504-6500, jherman@rgrdlaw.com

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)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. 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 District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION

(CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Class Action Fairness Act, 28 U.S.C. §1332(d)(2).

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 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 - "4" MONTHS DISCOVERY TRACK
- ☐ 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
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☑ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** $5,000,000+

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Not Assigned **DOCKET NO.** MDL No. 2800

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☑ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

/s/ John C. Herman — September 26, 2017

SIGNATURE OF ATTORNEY OF RECORD **DATE**