IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No.

JASON MORRIS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jason Morris (hereinafter "Plaintiff"), individually and on behalf of the class defined below, allege the following against Equifax, Inc. ("Equifax") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiff brings this class action case against Defendant Equifax for its failures to secure and safeguard consumers' personally identifiable information ("PII") which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate and adequate notice to Plaintiff and other class members that their PII had been stolen and precisely what types of information were stolen.

2. Equifax has acknowledged a cybersecurity incident ("Data Breach") potentially impacting approximately 143 million U.S. consumers. It has also acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, Equifax has admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personally identifiable information for approximately 182,000 U.S. consumers, were accessed.

3. Equifax has acknowledged that it discovered the unauthorized access on July 29, 2017, but delayed notification of the Data Breach to consumers. Instead, Equifax executives sold at least $1.8 million worth of shares before the public disclosure of the breach. It has been reported that its Chief Financial Officer John Gamble sold shares worth $946,374, its president of information solutions, Joseph Loughran, exercised options to dispose of stock worth $584,099, and its president of workforce solutions, Rodolfo Ploder, sold $250,458 of stock on August 2, 2017.

4. The PII for Plaintiff and the class of consumers he seeks to represent has been put at risk and was compromised due to Equifax's acts and omissions and their failure to properly protect the PII.

5. Equifax could have prevented this Data Breach. Data breaches at other companies, including one of its major competitors, Experian, have occurred. Equifax could have and should

have taken all necessary steps to prevent a breach, particularly given the amount of PII it held and its importance to each consumer for which it had the data.

6. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the PII that it collected during the course of its business.

7. Equifax disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening and failing to monitor and detect the breach on a timely basis.

8. As a result of the Equifax Data Breach, the PII of the Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered by Plaintiff and Class Members as a direct result of the Equifax Data Breach include:

a. Unauthorized use of their PII;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. Damages arising from the inability to use their PII;

e. Loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including

missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class Members' information on the Internet black market;

h. Damages to and diminution in value of their PII entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and

i. The loss of Plaintiff's and Class members' privacy.

9. The injuries to the Plaintiff and Class Members were directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for PII.

10. Further, Plaintiff and Class Members retain a significant interest in ensuring that their PII, which remains in the possession of Equifax, is protected from further breaches, and seek

to remedy the harms they have suffered on behalf of themselves and similarly situated consumers for whom the security of their PII was breached.

11. Plaintiff brings this action to remedy these harms on behalf of himself and all similarly situated individuals whose PII was available during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and Colorado Consumer Protection Act, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are thousands of putative class members. And, at least some members of the proposed Class have a different citizenship from Equifax.

13. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a), (b) and/or (c) because Plaintiff suffered injuries as a result of Defendant's acts in this District, a substantial number of the events giving rise to this Complaint occurred in this District and Defendant is authorized to conduct business in this District and has intentionally availed itself of the laws and markets of this District.

14. This Court has personal jurisdiction over Equifax because Equifax regularly conducts business in Colorado and has sufficient minimum contacts in Colorado.

PARTIES

15. Plaintiff Jason Morris is a resident of the State of Colorado. Plaintiff is harmed by the Data Breach.

16. Plaintiff Jason Morris has spent and will spend time and effort monitoring his financial accounts as a direct and proximate result of the Data Breach. Further, Plaintiff's PII has been put at a substantially increased risk of misuse requiring him to take protective measures he would not have had to take but for the breach. Any misuse of his data will result in additional damages to Plaintiff.

17. Defendant Equifax, Inc., is a Georgia corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax, Inc. may be served through its registered agent, Prentice-Hall Corp System, Inc., at 1560 Broadway, Suite 2090, Denver, CO 80202.

STATEMENT OF FACTS

18. Equifax is one of three nationwide credit-reporting companies that track and rates the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history. All this information, and more factors into credit scores.

19. Unlike other data breaches, not all of the people affected by the Equifax breach may be aware that they are customers of the company. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

20. According to Equifax's report on September 7, 2017, the breach was discovered on July 29th. The perpetrators gained access by "[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to retrieve "certain files."

21. Included among those files was a treasure trove of PII data: names, dates of birth, Social Security numbers and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.

22. PII like this is a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

23. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII – a form of intangible property that Plaintiff entrusted to Equifax and that was compromised in and as a result of the Equifax Data Breach.

24. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

25. Moreover, Plaintiff has a continuing interest in ensuring that his private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

26. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is highly sensitive,

susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud, and would be so used if obtained.

27. It is well-known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class Members.

28. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts or clone ATM, debit or credit cards.

29. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[1]

30. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data

[1] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci201 4.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).

security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

31. Equifax was fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Equifax's systems.

32. In spite of all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the PII of Plaintiff and Class Members was reckless or, at the very least, negligent.

33. The ramifications of Equifax's failure to keep Plaintiff's and Class Members' data secure are severe.

34. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[3]

35. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

[2] 17 C.F.R § 248.201 (2013).
[3] *Id.*
[4] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

36. Identity thieves can use personal information, such as that of Plaintiff and Class Members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

37. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[5]

38. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

39. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

---

[5] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).
[6] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).
[7] GAO, Report to Congressional Requesters, at 29 (June 2007), available at

40. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

41. The PII of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain Plaintiff's and Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

42. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

43. Equifax had the resources to prevent a breach, but failed to adequately invest in data security, despite the growing number of well-publicized data breaches.

44. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

---

http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

45. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's failure to secure their data, as is the case here.

46. Equifax's wrongful actions and inaction directly and proximately caused the risk of disclosure and acquisition of the PII of Plaintiff and Class Members, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation including, but not limited to:

a. Risk of theft of their personal and financial information;

b. Unauthorized charges on their debit and credit card accounts;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class Members' information on the black market;

d. The untimely and inadequate notification of the Data Breach;

e. The improper disclosure of their PII;

f. Loss of privacy;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

i. Ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. The loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, canceling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts,

and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

47. While the PII of Plaintiff and Members of the Class has been compromised, Equifax continues to hold PII of consumers, including Plaintiff and Class Members. Particularly because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

48. Plaintiff seeks relief on behalf of himself and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a class defined as follows:

> All persons residing in Colorado whose Personally Identifiable Information (PII) was held by Equifax from at least mid-May2017 through July 2017, including all persons who were affected by the Data Breach, and including all persons whom Equifax's "Check Potential Impact" tool identifies as being affected.

49. Excluded from the above class is Equifax and any of its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

50. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

51. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the Members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, the proposed Class includes hundreds of thousands individuals whose PII is maintained by Equifax. Class Members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

52. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Equifax had a duty to protect PII;

b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Equifax's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct constituted deceptive trade practices under Colorado law;

g. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

h. Whether Plaintiff and Class Members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its POS systems and data network; and,

i. Whether Plaintiff and Class Members are entitled to relief.

53. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class Members. Plaintiff had his PII put at risk by the Data Breach. Plaintiff's damages and injuries are akin to other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

54. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a Member of the Class and is committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

55. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify

individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

56. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

57. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Equifax failed to timely notify the public of the Breach;

b. Whether Equifax owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Equifax failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class Members; and,

f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

58. Finally, all members of the proposed Class are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and the consumers for whom it possesses data. Using this information, the Members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I
NEGLIGENCE

59. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

60. Upon gathering, accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and must be protected as private and confidential.

61. Equifax owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

62. Equifax owed numerous duties to Plaintiff and to Members of the Class including, but not limited to:

a. Exercising reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. Protecting PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. Implementing processes to quickly detect a data breach and to timely act on warnings about databreaches.

63. Equifax breached its duty to Plaintiff and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

64. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

65. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

66. Equifax breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate systems and data security practices to safeguard PII of Plaintiff and Class Members.

67. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class Members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

68. Equifax had a special and fiduciary relationship with Plaintiff and Class Members because Equifax held their PII. Plaintiff and Class Members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

69. Equifax's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

70. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class Members' Personal Information and promptly notify them about the data breach.

71. Equifax breached its duties to Plaintiff and Class Members in numerous ways including, but not limited to:

a. By failing to provide fair, reasonable, or adequate systems and data security practices to safeguard PII of Plaintiff and Class Members;

b. By creating a foreseeable risk of harm through the misconduct previously described;

c. By failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class Members' PII both before and after learning of the Data Breach;

d. By failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. By failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

72. Through Equifax's acts and omissions including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiff and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class Members during the time it was within Equifax possession or control.

73. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII. Equifax breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and Class Members and then by failing to provide Plaintiff and Class

Members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

74. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class Members during the time it was within Equifax's possession or control.

75. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Equifax prevented Plaintiff and Class Members from taking meaningful, proactive steps to monitor and secure their financial data and bank accounts.

76. Equifax's conduct was negligent and departed from reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and Class Members; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive PII had been or could be compromised.

77. Neither Plaintiff nor the other Class Members contributed to the Data Breach.

78. As a direct and proximate cause of Equifax's conduct, Plaintiff and the Class suffered damages and losses including, but not limited to: damages for inconvenience, time and annoyance of having to respond to the Data Breach, including monitoring their accounts; damages

for the increased risk of harm to their financial security and credit; damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; damages arising from Plaintiff's inability to use his debit or credit cards because those cards were canceled, suspended or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach including, but not limited to, late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
NEGLIGENCE PER SE

79. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

80. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

81. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiff and Class Members.

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

83. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

84. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

85. In addition, C.R.S. § 6-1-716(2) requires that:

> ". . . a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system."

86. Equifax negligently failed to meet the requirements of C.R.S. § 6-1-716(2) by failing to conduct a prompt investigation to determine the likelihood that the Plaintiff's and Class

Members' PII has been or will be misuses and by failing to give notice as soon as possible to Plaintiff and Class Members.

87. Equifax failure to meet the requirements of C.R.S. § 6-1-716(2) constitutes negligence per se.

88. Plaintiff and Class Members are within the class of persons that C.R.S. § 6-1-716(2) was intended to protect.

89. The harm that occurred as a result of the Equifax Data Breach is the type of harm C.R.S. § 6-1-716(2) was intended to guard against.

COUNT III
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")

90. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

91. As individuals, Plaintiff and Class Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

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

93. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

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

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

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

97. Equifax furnished the Class Members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities

and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

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

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

100. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties

under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other Class Members of their rights under the FCRA.

101. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and Class Members' PII for no permissible purposes under the FCRA.

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

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

COUNT IV
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

104. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

105. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well-aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

106. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the Class Members' PII and consumer reports for no permissible purposes under the FCRA.

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

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

109. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiff and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiff and Class Members.

COUNT V
DECLARATORY JUDGMENT

110. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

111. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Equifax to provide adequate security for the PII. As previously alleged, Equifax owes duties of care to Plaintiff and Class Members that require it to adequately secure PII.

112. Equifax still possesses PII pertaining to Plaintiff and Class Members.

113. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

114. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

115. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's obligations and duties of care to provide data security measures to Plaintiff and Class Members.

116. Plaintiff, therefore, seeks a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. Conducting regular database scanning and securing checks;

g. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

COUNT VI
VIOLATION OF COLORADO CONSUMER PROTECTION ACT
COLO. REV. STAT. § 6-1-105(1), *ET SEQ*.

117. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

118. Plaintiff and Class Members were consumers of Defendant's services and injured as result of Defendant's deceptive trade practices.

119. As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the Colorado Consumer Protection Act, including but not limited to by representing that its services were of a particular standard or quality that it knew or should have known were of another.

120. In addition, Equifax's failure to secure consumers' PII violated the FTCA and therefore violates the Colorado Consumer Protection Act.

121. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

122. As a direct and proximate result of Defendant's violation of the Colorado Consumer Protection Act, Plaintiff and Class Members are entitled to a judgment against Equifax for the greater of the amount of actual damages sustained or five hundred dollars or three times the amount of actual damages sustained and the costs of the action together with reasonable attorneys' fees pursuant to the Colorado Consumer Protection Act, to the extent allowed under the Act, and such other further relief as the Court deems just and proper.

COUNT VII
UNJUST ENRICHMENT

123. Plaintiff restates and realleges all preceding paragraphs as if fully set forth herein.

124. Plaintiff and Class Members conferred a monetary benefit on Equifax. Specifically, Equifax profited from and used the PII of Plaintiff and Class Members for business purposes. Equifax knew that Plaintiff and Class Members conferred a benefit on Equifax.

125. Equifax received the benefit of not incurring the cost of adequate and proper data security measures at the expense of Plaintiff and Class Members.

126. Equifax acquired the PII through inequitable means as it failed to disclose the inadequate security practices previously alleged.

127. Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on it and that Equifax received at the expense of Plaintiff and Class Members.

128. The Court should award as a remedy the expenditures saved and the profits obtained by Equifax at the expense of Plaintiff and the Class Members.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Equifax as follows:

a. For an Order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class Members;

c. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

This the 8th day of September, 2017.

/s/ Kevin S. Hannon
Kevin S. Hannon
Colorado Bar No. 16015
THE HANNON LAW FIRM, LLC
1641 Downing Street
Denver, CO 80218
(303) 861-8800
(303) 861-8855 - Fax
khannon@hannonlaw.com

/s/ Robert E. Caldwell, Jr.
Robert E. Caldwell, Jr.
Colorado Bar No. 47385
SAWAYA, ROSE, MCCLURE & WILHITE, P.C.
1600 Ogden Street
Denver, CO 80218
(303) 839-1650
(303) 832-7102 – Fax
RCaldwell@sawayalaw.com
Counsel for Plaintiffs and the Proposed Class