

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

JOSEPH CLARK, MEGHAN CLARK,  
and RUTH REYES, on behalf of  
themselves and all others similarly  
situated,

Plaintiffs,

v.

EQUIFAX INC.

Defendant.

Case No. \_\_\_\_\_

**COMPLAINT - CLASS ACTION**

Plaintiffs Joseph Clark, Meghan Clark, and Ruth Reyes (“Plaintiffs”), on behalf of themselves and all others similarly situated, allege as follows:

**NATURE OF THE CASE**

1. This is a data breach class action on behalf of 143 million consumers whose sensitive personal information including Social Security numbers, birth dates, names, addresses, and in some instances driver’s license numbers, credit card numbers, and other personal information (collectively “Personally Identifiable Information” or “PII”) was stolen from Defendant Equifax Inc. (“Equifax” or “Defendant”) in a cyber-attack.

2. Equifax failed to adequately safeguard consumers’ Personally

Identifiable Information. Lack of proper safeguards provided a means for unauthorized intruders to access Equifax's computer network and steal consumers' highly sensitive PII.

3. Armed with this sensitive information, data thieves can commit a variety of crimes including, *e.g.*, taking out loans in another person's name, opening new financial accounts in another person's name, using the victim's information to obtain government benefits, filing a fraudulent tax return using the victim's information, obtaining a driver's license in the victim's name but with another person's photograph, and giving false information to police during an arrest.

4. As a result of the breach, Plaintiffs and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft. Class members may be faced with fraudulent debt and may incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

5. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals whose PII was accessed during the breach.

6. Plaintiffs seek remedies including but not limited to compensatory damages, reimbursement of out-of-pocket costs, statutory damages under the Fair Credit Reporting Act (15 U.S.C. § 1681n(a)(1)(A)), credit monitoring services provided by a third party vendor unaffiliated with Equifax, and injunctive relief including improvements to Equifax's data security systems.

### **PARTIES**

7. Plaintiff Joseph Clark is domiciled in and a citizen of New Jersey. His personal information was compromised in the data breach. He checked the Equifax breach notification website and was informed by the automated system that his personal information was among the data compromised in the breach.

8. Plaintiff Meghan Clark is domiciled in and a citizen of New Jersey. Her personal information was compromised in the data breach. She checked the Equifax breach notification website and was informed by the automated system that her personal information was among the data compromised in the breach.

9. Plaintiff Ruth Reyes is domiciled in and a citizen of South Carolina. Her personal information was compromised in the data breach. She checked the Equifax breach notification website and was informed by the automated system that her personal information was among the data compromised in the breach.

10. Defendant Equifax Inc. is a citizen of Georgia. Its U.S. headquarters

and principal place of business are located at 1550 Peachtree Street, N.W., Atlanta, GA. Equifax, Inc. is incorporated in Georgia.

### **JURISDICTION & VENUE**

11. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds \$5,000,000 exclusive of interest and costs, and many members of the Class are citizens of states different from Defendant.

12. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because Plaintiffs are bringing claims under the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681e, *et seq.*

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is headquartered in this District and regularly transacts business here, and some of the Class members reside in this District. The causes of action arose, in part, in this District.

### **FACTS**

#### **I. Equifax’s Data Breach**

14. On September 7, 2017, Equifax issued a press release stating the following in relevant part:

Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately **143 million U.S. consumers**. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from **mid-May [2017] 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, 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 accessed**. . . .

. . . .

Equifax discovered the unauthorized access on July 29 of this year . . . .

. . . .

Equifax has established a dedicated website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers – all complimentary to U.S. consumers for one year.<sup>1</sup>

15. Equifax's breach announcement website stated that Equifax will not

---

<sup>1</sup> <https://www.equifaxsecurity2017.com/> (last visited Sept. 8, 2017) (emphasis added).

send direct mail notice to the vast majority of individuals affected by the breach.

Equifax stated:

Equifax will send direct mail notices to [only those] consumers whose credit card numbers or dispute documents with personal identifying information were impacted. . . .

. . . .

[For the remainder of the affected individuals, we] have provided a tool on this site for you to determine if your information was potentially impacted by this incident. To find out if you are potentially impacted, please go to [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), and click on “Potential Impact,” and enter your last name and last 6 digits of your Social Security number.<sup>2</sup>

16. Thus, affected individuals must submit part of their Social Security number to determine if they were impacted by the breach. Many Class members are likely uncomfortable doing so, and will forego an opportunity to learn if they were impacted by the breach. Other Class members might not be aware of this mechanism to determine if they were included in the breach. As a result, many Class members will not become aware that their sensitive PII is in the hands of cyber thieves.

17. The TrustedID credit monitoring product offered by Equifax is

---

<sup>2</sup> <https://www.equifaxsecurity2017.com/frequently-asked-questions/> (last visited Sept. 8, 2017).

administered by a subsidiary of Equifax. Equifax's data breach announcement did not disclose that TrustedID is administered by an affiliate. Thus, Class members are unaware that the credit monitoring product they are being offered is affiliated with the same entity whose deficient data security led to the data breach.

18. Attorneys General from multiple states including New York and Illinois are investigating Equifax's role in the breach.<sup>3</sup>

19. The New York Attorney General issued a statement stating: "Since Social Security numbers were affected, there is risk of tax fraud. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Consider filing your taxes early and pay close attention to correspondence from the IRS."<sup>4</sup>

20. The Illinois Attorney General urged affected consumers to place a credit freeze on their credit report in light of the "significant risk of identity theft posted by the breach."<sup>5</sup>

---

<sup>3</sup> <https://ag.ny.gov/press-release/ag-schneiderman-launches-formal-investigation-equifax-breach-issues-consumer-alert>; [http://www.illinoisattorneygeneral.gov/pressroom/2017\\_09/20170908.html](http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170908.html).

<sup>4</sup> <https://ag.ny.gov/press-release/ag-schneiderman-launches-formal-investigation-equifax-breach-issues-consumer-alert>.

<sup>5</sup> [http://www.illinoisattorneygeneral.gov/pressroom/2017\\_09/20170908.html](http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170908.html).

21. Equifax's breach announcement noted that credit reporting agencies may charge fees of up to \$10 to initiate, temporarily lift, or permanently remove credit freezes in certain states.<sup>6</sup> These fees constitute out-of-pocket losses to Class members.

22. Credit reporting agencies offer consumers one free credit report per year. Individuals who request more than one credit report per year must pay a fee for the additional report. These fees constitute out-of-pocket losses to Class members.

## **II. Equifax's Privacy Policy**

23. Equifax posted its privacy policy on its website. The policy stated, in relevant part: "We have built our reputation on our commitment to . . . protect the privacy and confidentiality of personal information about consumers. . . . Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."<sup>7</sup>

24. Equifax also made privacy representations in its public filings with the Securities and Exchange Commission. Equifax stated the following in its Form

---

<sup>6</sup> <https://www.equifaxsecurity2017.com/consumer-notice/> (last visited Sept. 7, 2017).

<sup>7</sup> <http://www.equifax.com/privacy/> (last visited Sept. 7, 2017).



10-K for the year ended December 31, 2016:

- “We continuously monitor federal and state legislative and regulatory activities that involve credit reporting, data privacy and security to identify issues in order to remain in compliance with all applicable laws and regulations.”<sup>8</sup>
- “The United States Fair Credit Reporting Act (‘FCRA’) regulates consumer reporting agencies, including us . . . . FCRA provisions govern the . . . privacy of information in the files of consumer reporting agencies (‘CRAs’) that engage in the practice of assembling or evaluating certain information relating to consumers for certain specified purposes.”<sup>9</sup>
- “We are subject to a number of U.S. and state . . . laws and regulations relating to consumer privacy, data and financial protection. These regulations are complex . . . [and] have tended to become more stringent over time . . . .”<sup>10</sup>

---

<sup>8</sup> <https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?FilingId=11875154&Cik=0000033185&Type=PDF&hasPdf=1>, at pg. 11.

<sup>9</sup> *Id.* at pg. 10.

<sup>10</sup> *Id.* at pg. 17.

25. These representations illustrate some of the various duties imposed on Equifax to adequately safeguard consumer information.

26. The implication from these privacy disclosures was that Equifax could and would adequately safeguard consumer data.

### **III. Damages**

27. Plaintiffs and Class members face a substantial risk of out of pocket fraud losses such as, *e.g.*, loans opened in their names, tax return fraud, utility bills opened in their name, credit card fraud, and similar identity theft.

28. Plaintiffs and Class members may incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the breach.

29. Plaintiffs and Class members are entitled to statutory damages of \$100 to \$1,000 per person pursuant to the FCRA, 15 U.S.C. § 1681n(a)(1)(A).

30. Plaintiffs and Class members suffered a loss of value of their sensitive Personally Identifiable Information when it was acquired by cyber thieves in the data breach.

31. Plaintiffs and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts for misuse.

## CLASS ACTION ALLEGATIONS

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

### **A. Nationwide Class**

33. Plaintiffs bring their negligence claim (Count I) and FCRA claims (Counts II and III) on behalf of a proposed nationwide class (“Nationwide Class”), defined as follows:

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

### **B. Statewide Subclasses**

34. Plaintiffs bring certain claims on behalf of subclasses of residents of New Jersey (the “New Jersey Subclass”) and/or South Carolina (the “South Carolina Subclass”).

35. The New Jersey Subclass is defined as follows:

All natural persons and entities residing in New Jersey whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

36. The South Carolina Subclass is defined as follows:

All natural persons and entities residing in South Carolina whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

37. Specifically, Plaintiffs bring their negligence claim (Count I) on behalf of the New Jersey Subclass and South Carolina Subclass, in the alternative to bringing that claim on behalf of the Nationwide Class.

38. Plaintiffs Joseph Clark and Meghan Clark bring their New Jersey consumer protection claim (Count IV) and New Jersey data breach notification statute claim (Count V) on behalf of the New Jersey Subclass only.

39. Plaintiff Ruth Reyes brings her South Carolina data breach notification statute claim (Count VI) on behalf of the South Carolina Subclass only.

40. Except where otherwise noted, “Class members” shall refer to members of the Nationwide Class, New Jersey Subclass, and South Carolina Subclass, collectively. “Class” shall refer to the Nationwide Class, New Jersey Subclass, and South Carolina Subclass, collectively.

41. Excluded from the Class is Defendant and its current employees.

42. The Class is so numerous that joinder of all members is impracticable. The Nationwide Class includes approximately 143 million individuals whose PII was compromised in the data breach. The New Jersey Subclass and South

Carolina Subclass each include millions or hundreds of thousands of individuals whose PII was compromised in the data breach.

43. There are various questions of law and fact common to Plaintiffs and the Class, including but not limited to the following:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant owed a duty to Plaintiffs and Class members to adequately protect their personal information;
- whether Defendant breached its duties to protect personal information of Plaintiffs and Class members;
- whether Defendant knew or should have known that its data security systems and processes were vulnerable to attack;
- whether Defendant violated the FCRA;
- whether Defendant unreasonably delayed providing notice of the breach to Class members;
- whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's conduct; and
- whether Plaintiffs and Class members are entitled to injunctive relief.

44. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class members, had their personal information compromised in

the data breach.

45. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation.

46. Plaintiffs have no interests that are adverse to, or in conflict with, the Class.

47. Questions of law and fact common to the Class predominate over any questions which may affect only individual Class members.

48. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation.

49. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy.

50. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the

parties' resources, and protects the rights of each class member.

51. Defendant has acted on grounds that apply generally to the Class, so that injunctive relief is appropriate with respect to the Class as a whole under Fed. R. Civ. P. 23(b)(2).

**COUNT I  
NEGLIGENCE  
(BROUGHT ON BEHALF OF THE NATIONWIDE CLASS,  
NEW JERSEY SUBCLASS, AND SOUTH CAROLINA SUBCLASS)**

52. Plaintiffs incorporate by reference the paragraphs set out above as if fully set forth herein.

53. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, and safeguarding their sensitive PII. This duty included, among other things, designing, maintaining, monitoring, and testing Defendant's security systems and procedures to ensure that Class members' information was adequately secured.

54. Defendant owed a duty to Class members to implement intrusion detection processes that would detect a data breach in a timely manner.

55. Defendant also had a duty to delete any personal information that was no longer needed to serve client needs.

56. Defendant's privacy policy and disclosures in its Form 10-K acknowledged Defendant's duty to adequately protect consumers' personal

information.

57. Defendant owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class members' PII.

58. Defendant breached its duties by, among other things: (a) failing to maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the data breach in a timely manner; and (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Class members' PII.

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

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

61. Damages to Plaintiffs and Class members were caused by, and a proximate result of, Defendant's breaches of its duties.

62. Plaintiffs and Class members suffered various types of damage as set forth above.



**COUNT II**  
**WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT**  
**(BROUGHT OF BEHALF OF THE NATIONWIDE CLASS)**

63. Plaintiffs incorporate by reference the paragraphs set out above as if fully set forth herein.

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

65. 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).

66. 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.

67. 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).

68. 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).

69. The compromised data was partly or wholly a consumer report under the FCRA because it was 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.

70. 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

Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

71. Equifax furnished Class members' consumer reports by disclosing the 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.

72. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the [FCRA]," in connection with data breaches.<sup>11</sup>

73. 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.

---

<sup>11</sup> See Statement of Commissioner Brill (Federal Trade Commission 2011), available at <https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonstatement.pdf>.

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

75. 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 depriving Plaintiffs and Class members of their rights under the FCRA.

76. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain Plaintiffs' and Class members' PII for no permissible purposes under the FCRA.

77. Plaintiffs and Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each individual Class member 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) (emphasis added).

78. Plaintiffs and 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 III**  
**NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**  
**(BROUGHT ON BEHALF OF THE NATIONWIDE CLASS)**

79. Plaintiffs incorporate by reference the paragraphs set out above as if fully set forth herein.

80. 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.

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

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

83. Plaintiffs and 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).

**COUNT IV**  
**NEW JERSEY CONSUMER FRAUD ACT,**  
**N.J. STAT. ANN. § 56:8-1, et. seq.**  
**(BROUGHT ON BEHALF OF THE NEW JERSEY SUBCLASS)**

84. Plaintiffs incorporate by reference the paragraphs set out above as if fully set forth herein.

85. Plaintiffs Joseph Clark and Meghan Clark bring this claim against Defendant on behalf of the New Jersey Subclass.

86. Defendant sells “merchandise,” as defined by N.J. Stat. Ann. § 56:8-1(c) to include “goods” and “services,” by offering credit report and credit monitoring products and services to the public.

87. Defendant engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the provision of credit report and credit monitoring services in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

- a. Defendant misrepresented material facts, pertaining to the provision of credit report and credit monitoring services, to the New Jersey Subclass by representing that Defendant would maintain adequate data privacy practices and procedures to

safeguard consumers' personal information from unauthorized disclosure, release, data breaches, and theft;

- b. Defendant misrepresented material facts pertaining to the provision of credit report and credit monitoring services to the New Jersey Subclass by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to data privacy and security;
- c. Defendant knowingly omitted the material fact of the inadequacy of its privacy and security protections for consumers' personal information with the intent that others rely on the omission, suppression, and concealment, regardless of whether others did in fact rely on the omission;
- d. Defendant engaged in unconscionable and deceptive acts and practices with respect to the provision of credit report and credit monitoring services by failing to maintain the privacy and security of New Jersey Subclass members' personal information, in violation of duties imposed by applicable federal and state laws and Defendant's own privacy representations; and
- e. Defendant engaged in unconscionable and deceptive acts and

practices with respect to the provision of credit report and credit monitoring services by failing to disclose the data breach to New Jersey Subclass members in a timely and effective manner, in violation of N.J. Stat. Ann. § 56:8-163(a).

88. These unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

89. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

90. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard New Jersey Subclass members' personal information and that the risk of a data breach was unreasonably high. Defendant's actions in engaging in the above unfair practices and deceptive acts were knowing, willful, reckless, and/or negligent with respect to the rights of New Jersey Subclass members.

91. As a direct and proximate result of Defendant's unconscionable or deceptive acts and practices, New Jersey Subclass members suffered an "ascertainable loss of money or property" pursuant to N.J. Stat. Ann. § 56:8-19, including the loss of their legally protected interest in the confidentiality and



privacy of their personal information.

92. New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to actual damages, treble damages, equitable relief, and attorneys' fees and costs.

**COUNT V**  
**VIOLATION OF THE NEW JERSEY DATA BREACH**  
**NOTIFICATION STATUTE, N.J.S.A. 56:8-163**  
**(BROUGHT ON BEHALF OF THE NEW JERSEY SUBCLASS)**

93. Plaintiffs incorporate by reference the paragraphs set out above as if fully set forth herein.

94. Defendant was required to timely notify New Jersey Subclass members of the breach following Defendant's discovery of the breach. The New Jersey data breach notification statute states that an entity "that conducts business in New Jersey . . . shall disclose any breach of security of [its] computerized records following discovery . . . of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person." N.J.S.A. 56:8-163(a).

95. The disclosure "shall be made in the most expedient time possible and without unreasonable delay." N.J.S.A. 56:8-163(a).

96. Class members' PII (e.g., Social Security numbers) includes personal information as defined by N.J.S.A. 56:8-161.

97. Defendant unreasonably delayed providing notice of the breach. Defendant discovered the breach on July 29, 2017, but did not publicly disclose the breach until nearly six weeks later on September 7, 2017. Defendant could and should have provided notice sooner.

98. Defendant's primary notification system involved mere website notice, which could have been implemented more quickly. Website notice does not involve any of the logistical delays that would accompany a direct-mail campaign for millions of Class members.

99. Also, on August 1-2, 2017, just three days after the breach was discovered and several weeks before it was made public, at least three Equifax executives sold at least \$1.8 million worth of Equifax shares of stock.<sup>12</sup> If these executives knew the severity of the breach after just three days, and had time to try to beat the market with stock sales, Equifax should have had time to provide public notice of the breach before waiting several more weeks to do so.

100. As a direct and proximate result of Defendant's violation of N.J.S.A. 56:8-163(a), New Jersey Subclass members suffered damages as described above. New Jersey Subclass members were harmed because, *e.g.*, they were deprived of

---

<sup>12</sup> <http://money.cnn.com/2017/09/08/investing/equifax-stock-insider-sales-hack-data-breach/>.

an opportunity to monitor their financial and other accounts sooner and more promptly enact protective measures such as credit monitoring and credit freezes.

101. Defendant's delay in notifying New Jersey Subclass members of the breach was unjustified.

102. Plaintiffs and New Jersey Subclass members are entitled to damages for Defendant's violation of N.J.S.A. 56:8-163(a).

**COUNT VI  
VIOLATION OF THE SOUTH CAROLINA DATA BREACH  
NOTIFICATION STATUTE, S.C. CODE ANN. § 39-1-90(A)  
(BROUGHT ON BEHALF OF THE SOUTH CAROLINA SUBCLASS)**

103. Plaintiffs incorporate by reference the paragraphs set out above as if fully set forth herein.

104. Defendant was required to timely notify South Carolina Subclass members of the breach following Defendant's discovery of the breach. The South Carolina data breach notification statute states that an entity "conducting business in this State . . . shall disclose a breach of the security of [its] system following discovery . . . of the breach in the security of the data to a resident of this State." S.C. Code Ann. § 39-1-90(A).

105. The disclosure must be made "in the most expedient time possible and without unreasonable delay." S.C. Code Ann. § 39-1-90(A).

106. Defendant is a business that owns or licenses computerized data or

other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

107. Class members' PII (e.g., Social Security numbers) includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(D)(3).

108. Defendant unreasonably delayed providing notice of the breach. Defendant discovered the breach on July 29, 2017, but did not publicly disclose the breach until nearly six weeks later on September 7, 2017. Defendant could and should have provided notice sooner.

109. Defendant's primary notification system involved mere website notice, which could have been implemented more quickly. Website notice does not involve any of the logistical delays that would accompany a direct-mail campaign for millions of Class members.

110. Also, on August 1-2, 2017, just three days after the breach was discovered and several weeks before it was made public, at least three Equifax executives sold at least \$1.8 million worth of Equifax shares of stock.<sup>13</sup> If these executives knew the severity of the breach after just three days, and had time to try to beat the market with stock sales, Equifax should have had time to provide public

---

<sup>13</sup> <http://money.cnn.com/2017/09/08/investing/equifax-stock-insider-sales-hack-data-breach/>.

notice of the breach before waiting several more weeks to do so.

111. As a direct and proximate result of Defendant's violation of S.C. Code Ann. § 39-1-90(A), South Carolina Subclass members suffered damages as described above. South Carolina Subclass members were harmed because, *e.g.*, they were deprived of an opportunity to monitor their financial and other accounts sooner and more promptly enact protective measures such as credit monitoring and credit freezes.

112. Defendant's delay in notifying South Carolina Subclass members of the breach was willful, knowing, and/or negligent under S.C. Code Ann. § 39-1-90(G).

113. Plaintiffs and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including but not limited to actual damages, injunctive relief, attorneys' fees, and costs.

### **RELIEF REQUESTED**

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Equifax as follows:

A. An award to Plaintiffs and the Class of compensatory, statutory, consequential, and incidental damages;

B. An award of credit monitoring and identity theft protection services

beyond the one-year package Equifax is currently offering, to be provided by an entity unaffiliated with Equifax;

C. Injunctive relief requiring Equifax to strengthen its data security systems and submit to future periodic audits;

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

E. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

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

### **JURY TRIAL DEMAND**

Plaintiffs demand a jury trial on all issues so triable.

Dated: September 12, 2017

Respectfully submitted,

/s/ E. Michelle Drake

**BERGER & MONTAGUE, P.C.**

E. Michelle Drake (GA Bar No. 229202)

43 SE Main Street, Suite 505

Minneapolis, MN 55414

Tel: (612) 594-5933

Fax: (612) 584-4470

emdrake@bm.net

**BERGER & MONTAGUE, P.C.**

Sherrie Savett (pro hac vice forthcoming)

Shanon Carson (pro hac vice forthcoming)

Jon Lambiras (pro hac vice forthcoming)

1622 Locust St.  
Philadelphia, PA 19103  
Tel: (215) 875-3000  
Fax: (215) 875-4604  
ssavett@bm.net  
scarson@bm.net  
jlambiras@bm.net

*Counsel for Plaintiffs and the Class*

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)

Joseph Clark, Meghan Clark, and Ruth Reyes, on behalf of themselves and all others similarly situated.

DEFENDANT(S)

Equifax Inc.

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF New Jersey (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)

E. Michelle Drake, Berger & Montague, P.C., 43 SE Main Street, Suite 505, Minneapolis, MN 55414, Tel: (612) 594-5933, Email: emdrake@bm.net.

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION (PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF, 2 U.S. GOVERNMENT DEFENDANT, 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY), 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 1 CITIZEN OF THIS STATE, 2 CITIZEN OF ANOTHER STATE, 3 CITIZEN OR SUBJECT OF A FOREIGN COUNTRY, 4 INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE, 5 INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE, 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 complaint for violation of the Fair Credit Reporting Act (15 U.S.C. § 1681e, et seq.), Negligence, and violation of several state statutes arising from a data breach.

(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 (Referral), NATURE OF SUIT, CAUSE OF ACTION



**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 (1395f)
- 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 ANTI-TRUST
- 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 \$ Greater than \$5 million

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

**VIII. RELATED/REFILED CASE(S) IF ANY**

JUDGE Hon. William S. Duffey DOCKET NO. 17-cv-03422

**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/E. Michelle Drake

9/12/2017

SIGNATURE OF ATTORNEY OF RECORD

DATE