

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

RODD SANTOMAURO,  
*Individually and on behalf of  
all others similarly situated*  
1151 4<sup>th</sup> Street SW  
PH 21  
Washington, DC 20024

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

- AND -

**CLASS ACTION COMPLAINT**

BRENDA BIRKETT,  
*Individually and on behalf of  
all others similarly situated*  
2550 Finzel Road  
Frostburg, MD 21532

**JURY DEMAND**

- AND -

DEBRA LEE,  
*Individually and on behalf of  
all others similarly situated*  
102 Williamsburg Way  
Nitro, WV 25143

Plaintiffs,

v.

EQUIFAX INC.  
1550 Peachtree Street NW, H46  
Atlanta, GA 30309-2402

**Serve:**  
**Prentice-Hall Corporation**  
**System Inc., 1090 Vermont Ave.**  
**NW, Washington DC 20005**

**CLASS ACTION COMPLAINT**

Plaintiffs Rodd Santomauro, Brenda Birkett, and Debra Lee make this class action complaint against Defendant Equifax Inc. (hereinafter “Defendant” or “Equifax”); and for their claims state the following:

**PARTIES**

1. Plaintiff Rodd Santomauro is an adult resident of the District of Columbia.
2. Plaintiff Brenda Birkett is an adult resident of the State of Maryland.
3. Plaintiff Debra Lee is an adult resident of the State of West Virginia.
4. Defendant Equifax Inc. is a foreign corporation doing business in the District of Columbia. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC a/k/a Equifax Personal Solutions a/k/a PSOL. Each of these entities acted as agents of Equifax, or in the alternative, acted in concert with Equifax as alleged in this Complaint.

**JURISDICTION**

5. Each of the preceding paragraphs is incorporated by reference herein.
6. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) in that Plaintiffs file their claims as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and that in the aggregate the claims and claims of the other members of the Class exceed \$5,000,000 exclusive of interests and costs, and there are numerous class members who are citizens of states other than the Defendant.
7. This Court has personal jurisdiction over the Defendant because the Defendant is authorized to do business in the District of Columbia, and offer and/or sell credit reporting and credit monitoring products to citizens of the District of Columbia.
8. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because the acts and transactions giving rise to this action occurred in this District and because the Defendant is subject to personal jurisdiction in this District.

**SUMMARY OF THE CASE**

9. Each of the preceding paragraphs is incorporated by reference herein.

10. This is a class action lawsuit brought by Plaintiffs, individually and on behalf of all others similarly situated, due to the failure of Defendant to safeguard and secure personally identifiable information including social security numbers, names, addresses, credit worthiness information, credit card numbers, and, possibly other highly confidential information and personal related information<sup>2</sup> of Plaintiffs and Class Members.
11. Defendant announced to the public a massive loss of information on September 7, 2017, wherein the Plaintiffs personal “PII” and “Sensitive Information,” that was to be protected and entrusted to Defendant was stolen and/or made accessible to hackers and identity thieves.
12. As a result of Defendant’s failure to implement and follow basic security procedures, the PII/Sensitive Information of a multitude of residents of the District of Columbia, the State of Maryland, and the State of West Virginia, including the Plaintiffs and the class they seek to represent, is now in the hands of thieves.
13. The Plaintiffs and Class Members now face an increased risk of identity theft, if not actual identity theft and resulting losses, and need to take immediate action to protect themselves from identity theft, which has already resulted and will continue to result in real and actual loss regardless of whether identity theft actually occurs.
14. Plaintiffs and Class Members are immediately and imminently in danger of sustaining some or further direct injury/injuries as a result of the identity theft they suffered when Defendant did not protect and secure their PII/Sensitive Information and disclosed their PII/Sensitive Information to hackers. These further instances of identity theft are certainly impending and imminent. The PII/Sensitive Information accessed, copied, and

---

<sup>2</sup> (Collectively, “Personally Identifiable Information” or “PII;” and “Sensitive Information”)

transferred from Defendant have all of the information wrongdoers need, and the American government and financial systems requires, to completely and absolutely misuse Plaintiffs' and Class Members' identity to their detriment.

15. Consequently, the Plaintiffs and Class Members have or will have to spend significant time and money to protect themselves; including, but not limited to: the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, cost of conducting a damage assessment, mitigation costs, costs to rehabilitate Plaintiffs' and Class Members' PII/Sensitive Information, and costs to reimburse from losses incurred as a proximate result of the breach.
16. Many Plaintiffs and Class Members suffered from actual economic injury resulting in direct economic harm as a result of the identity theft they suffered when Defendant did not protect and secure their PII/Sensitive Information and disclosed their PII/Sensitive Information to hackers.
17. Many Plaintiffs contracted for services that included a guarantee by Defendant to safeguard and/or monitor their personal information and, instead, Plaintiffs received services devoid of these very important protections. Accordingly, Plaintiffs allege claims for breach of contract, unlawful trade practices, unjust enrichment, negligence, and negligence *per se*.

**FACTS COMMON TO ALL CLAIMS**

18. Each of the preceding paragraphs is incorporated by reference herein.
19. Equifax collected and stored the PII and Sensitive Information of Brenda Birkett, Rodd Santomauro, and Debra Lee, including their social security numbers, birth dates, home addresses, credit worthiness information, and credit card numbers.

20. Equifax also collected and stored the PII and Sensitive Information of millions of consumers including their social security numbers, birth dates, home addresses, credit worthiness information, and credit card numbers.
21. Equifax undertook the care of PII, Sensitive Information, and credit and personal information belonging to Plaintiffs and the putative class, then breached its legal duty by failing to maintain adequate technological safeguards, falling below the standard of care in the technological industry, directly and proximately causing foreseeable risk of data loss and credit harm and identity theft and other economic losses.
22. Plaintiffs and the class are entitled to equitable relief in the form of an accounting of exactly how their credit and personal information was accessed without authorization by third parties, restitution, and unless agreed upon by Equifax, an Order to preserve all documents and information (and electronically stored information) pertaining to this case.
23. Plaintiffs file this complaint as a national class action on behalf of over 140 million consumers across the United States harmed by Equifax's failure to adequately protect their credit and personal information.
24. This complaint further requests that Equifax provide fair compensation in an amount that will ensure every consumer harmed by its data breach will not suffer from out-of-pocket losses for the costs of independent third-party credit repair and monitoring services.
25. Equifax owed a legal duty to consumers like Brenda Birkett, Rodd Santomauro, and Debra Lee to use reasonable care to protect their credit and personal information from unauthorized access by third parties. Equifax knew that its failure to protect Brenda Birkett, Rodd Santomauro, and Debra Lee's credit and personal information from unauthorized access would cause serious risks of credit harm and identity theft for years to come.

26. Plaintiffs and members of The Class have suffered economic and non-economic loss in the form of mental and emotional pain and suffering and anguish as a result of Defendant's failures.
27. On September 7, 2017, Equifax announced for the first time that from May to July 2017, its database storing Brenda Birkett, Rodd Santomauro, and Debra Lee's credit and personal information had been hacked by unauthorized third parties, subjecting these consumers to credit harm and identity theft.
28. By failing to provide the appropriate technology safeguards that Defendant's privacy policies indicated, the cyberattack allowed access to PII and other personal and Sensitive Information of Plaintiffs and class members.
29. Equifax failed to timely recognize that a cyberattack was occurring, invading the Sensitive Information of more than one hundred million (100,000,000) individuals.
30. Finally, on September 7, 2017 - months after the cyberattack occurred - Defendant notified Plaintiffs and the class members that a cyberattack had occurred and that some of their personal information may have been gathered by individuals with ulterior motives.
31. In an attempt to increase profits, Equifax negligently failed to maintain adequate technological safeguards to protect Brenda Birkett, Rodd Santomauro, and Debra Lee's information from unauthorized access by hackers. Equifax knew and should have known that failure to maintain adequate technological safeguards would eventually result in a massive data breach.
32. Equifax experienced previous data breaches and failed to sufficiently improve its cyber security in response to those failures.
33. Equifax could have and should have substantially increased the amount of money it spent to protect against cyber-attacks but chose not to. Consumers like Brenda Birkett, Rodd

Santomauro, and Debra Lee should not have to bear the expense caused by Equifax's negligent failure to safeguard their credit and personal information from cyber-attackers.

34. As a direct result of Equifax's conduct as alleged in this complaint many of the Plaintiffs, including Rodd Santomauro, suffered a loss of money by being forced to pay for third-party credit monitoring services they otherwise would not have had to pay for.
35. The consumers comprised in the putative class as alleged in this complaint suffered injury directly and proximately caused by Equifax's negligent failure to adequately protect its database from unauthorized access by third-party hackers.
36. Many Plaintiffs are customers of Equifax, and provided payment to Defendant for certain services, including credit monitoring and credit information services. These Plaintiffs did not get the benefit of their bargain and payment which was intended to pay administrative costs of securing their PII/Sensitive Information.
37. Many Plaintiffs contracted for services that included a promise by Equifax to safeguard, protect, monitor, and not disclose their personal information and instead, Plaintiffs received services devoid of these very important protections.
38. Personal Information is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
39. Despite Defendant's stated privacy policy, Defendant did not provide proper cyber security protecting the PII whether in transit or at rest, which the Plaintiffs and class members provided to Defendant.
40. The unauthorized access and breach to said combination of information creates a material risk of identity theft and access to other personal information including Personal Identification Information, financial information, and other Sensitive Information.

### CONSEQUENCES OF DEFENDANT'S CONDUCT

41. Each of the preceding paragraphs is incorporated herein.
42. The ramifications of Defendant's failure to keep class members' PII and other personal and Sensitive Information secure are severe.
43. Identity thieves can use identifying data - including that accessed on Defendant's servers - to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.
44. Identity thieves can use personal information such as that pertaining to the Class, which Defendant failed to keep secure to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the 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.
45. In addition, identity thieves may get medical services using the Plaintiff's PII or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.
46. Annual monetary losses from identity theft are in the billions of dollars. The Presidential Report on identity theft points out the following:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and



frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, at p.11 (April 2007), available at: <<http://www.ftc.gov/sites/default/files/documents/reports/combating-identitytheft-strategic-plan/strategicplan.pdf>> (last visited Sept. 9, 2017).

47. 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.

GAO, *Report to Congressional Requesters*, at p.29 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (last visited Sept. 9, 2017).

48. With the advent of the prescription drug benefit of Medicare Part D, the Department of Health and Human Services' Office of the Inspector General (HHS OIG) has noted a growing incidence of health care frauds involving identity theft. Identity thieves can use such information "fraudulently to enroll unwilling beneficiaries in alternate Part D plans in order to increase . . . sales commissions" or commit other types of fraud. "The types of fraud that can be perpetrated by an identity thief are limited only by the ingenuity and resources of the criminal." *Id.* at 31.

49. Plaintiffs and the class they seek to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.
50. Plaintiffs Brenda Birkett, Rodd Santomauro, and Debra Lee had their PII disclosed as a result of the Defendant's failures to protect their information. Equifax promised that their information would be protected in accordance with industry standards and as mandated by law.
51. As a result of Defendant failing to protect the Plaintiffs' PII//Sensitive Information, many Plaintiffs have already suffered from direct economic injury such as missing work to address the breach of their information, purchasing credit monitoring, identify theft, credit card fraud, and other conduct causing direct economic injury.

### **CLASS ACTION ALLEGATIONS**

52. Pursuant to Rule 23 - specifically Rule 23(b)(1), 23(b)(2) and 23(b)(3) - of the Federal Rules of Civil Procedure, the Plaintiffs bring this action on their own behalf, and on behalf of all other persons similarly situated ("the Class").
53. The Class that Plaintiffs seek to represent the following class and subclasses:

#### **THE CLASS**

All persons who reside in the District of Columbia, the State of Maryland and West Virginia whose personally identifiable information, sensitive personal information, and/or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.<sup>3</sup>

#### **THE SUBCLASSES**

1. All persons who reside in the District of Columbia whose personally identifiable information, sensitive personal information, and/or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.<sup>4</sup>

---

<sup>3</sup> Hereinafter referred to as "The Class."

<sup>4</sup> Hereinafter referred to as "The DC Class" or "The DC Subclass."

2. All persons who reside in the State of Maryland whose personally identifiable information, sensitive personal information, and/or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.<sup>5</sup>
  3. All persons who reside in West Virginia whose personally identifiable information, sensitive personal information, and/or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.<sup>6</sup>
54. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendant.
55. Excluded from the Classes are (i) any judge presiding over this action and members of their families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and their current or former employees, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Classes; and (iv) the legal representatives, successors, or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of the data stored by Defendant.
56. Plaintiffs meet the requirements of Federal Rules of Civil Procedures 23(a) because the members of The Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is in excess of one hundred and forty million (140,000,000) individuals whose information is now in the hands of thieves.
57. Plaintiffs meet the requirements of Federal Rules of Civil Procedures 23(a) because there is a well-defined community of interest among the members of The Class, common

---

<sup>5</sup> Hereinafter referred to as "The Maryland Class" or "The Maryland Subclass."

<sup>6</sup> Hereinafter referred to as "The West Virginia Class" or "The West Virginia Subclass."

questions of law and fact predominate, the claims are typical of the members of The Class, and the Plaintiffs can fairly and adequately represent the interests of The Class.

58. The action satisfies the requirement of Federal Rule of Civil Procedure 23(b)(1) because prosecuting separate actions by or against individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class; or adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests

59. Plaintiffs and members of The Class also seek injunctive relief because Defendant has acted and failed to act on grounds that affect The Class as a whole. Therefore, the action satisfies the requirements of Rule 23(b)(2).

60. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(3) because it involves questions of law and fact common to the member of The Class that predominate or any questions affecting only individual members, including, but not limited to:

- a. Whether the Defendant unlawfully used, maintained, lost or disclosed Class members' PII and Sensitive Information;
- b. Whether the Defendant unreasonably delayed in notifying affected individuals of the data breach;
- c. Whether the Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;
- d. Whether the Defendant's conduct was negligent;

- e. Whether the Defendant's conduct was a breach of contract;
  - f. Whether the Defendant violated applicable consumer protection statutes;
  - g. Whether the Defendant violated applicable Data Breach Notification statutes;
  - h. Whether the Defendant committed fraud;
  - i. Whether the Defendant were unjustly enriched;
  - j. Whether the Defendant breached their duties of confidentiality; and,
  - k. Whether the Plaintiffs and The Class are entitled to damages, statutory penalties, punitive damages, and/or injunctive relief.
58. The Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by the Defendant.
59. Plaintiffs will fairly and adequately represent the interests of The Class and the respective subclasses.
60. The prosecution of separate actions by individual members of The Class or separate actions of each subclass would create a risk of inconsistent or varying adjudications with respect to individual members of The Class, which would establish incompatible standards of conduct for the Defendant and would lead to repetitive adjudication of common questions of law and fact. The Class is in excess of 1 million (1,000,000) individuals, and accordingly, class treatment is superior to any other method for adjudicating the controversy. The Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action under Rule 23(b)(3).
61. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, the Defendant's violations of

law inflicting substantial damages in the aggregate would go un-remedied without certification of The Class.

62. For all of the foregoing reasons, certification is proper under Rule 23(b)(1), 23(b)(2) and 23(b)(3).

63. Plaintiffs reserve the right to revise Class definitions and questions based upon facts learned in discovery.

**NEGLIGENCE**  
**Count I**

64. Each of the preceding paragraphs is incorporated herein.

65. Defendant owed the Plaintiffs a duty of care in protecting the confidentiality of the personal and private information of the Plaintiffs provided to the Defendant.

66. Defendant came into possession of Plaintiffs' PII and Sensitive Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

67. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' PII and Sensitive Information.

68. Defendant had a duty to conduct audits of its electronic files and determine whether any PII or Sensitive Information had been obtained by unauthorized parties.

69. Defendant had a duty to provide reasonable and timely notice to Plaintiffs and members of The Class regarding the data breach and the steps that can be taken by Plaintiffs and members of the Class to protect themselves from identity theft.

70. The Defendant was negligent in that it breached the duty of reasonable care that it owed to the Plaintiffs by failing to have in place reasonable and appropriate protections from unauthorized data breaches, by failing to provide a reasonable and

timely notice of a breach, and by failing to perform reasonable and timely audits of the data protection system.

71. As a direct and proximate result of the Defendant's negligence, the Plaintiffs have suffered damages, including pain and suffering and past and future economic loss.

72. **WHEREFORE**, Plaintiffs demand judgment against Defendant for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorneys' fees.

**BREACH OF CONTRACT (express and implied)**

**Count II**

73. Each of the preceding paragraphs is incorporated herein.

74. Many Plaintiffs and class members paid money to Defendant in exchange for credit monitoring and credit information products, which included promises to protect Plaintiffs' PII and Sensitive Information.

75. Defendant promised Plaintiffs and the class members that Defendant would protect Plaintiffs' Sensitive Information.

76. To the extent that it was not expressed, an implied contract was created whereby Defendant promised to safeguard Plaintiffs' Sensitive Information from being accessed, copied, and transferred by third parties.

77. Under the contract, Defendant was further obligated to provide Plaintiffs with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

78. Defendant did not safeguard Plaintiffs' PII and Sensitive Information; therefore, Defendant breached its contract with Plaintiffs.

79. Furthermore, Defendant's failure to satisfy its confidentiality and privacy obligations resulted in Defendant providing services to Plaintiffs that were of a diminished value.

80. As a result, Plaintiffs have been harmed and/or injured and will incur economic and non-economic damages as a proximate and direct result of the breach by Defendant.

**WHEREFORE**, Plaintiffs demand judgment against Defendant for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorneys' fees.

**VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER PROTECTION ACT**

**Count III**

81. Each of the preceding paragraphs is incorporated by reference herein.

82. Defendant produced a privacy policy representing to Plaintiff Rodd Santomauro and members of the DC Class and the DC General Public that personal information which Defendant had in its possession and control would be secured by appropriate means of encryption on Defendant's electronic computers and servers.

83. Instead, Defendant failed to secure the personal information that Plaintiff Rodd Santomauro and the DC Class, allowing that information to be stored without the security safeguards and benefits of appropriate levels of encryption.

84. As such, Defendant violated its privacy policy and committed an unfair and unlawful trade practice in that the services provided:

- a. Did not provide the types of characteristics and benefits which Defendant proffered when Defendant claimed to protect the PII of the class members;
- b. Misrepresented as to a material fact which has a tendency to mislead because Defendant did not properly secure the PII as indicated in its privacy policy;



- c. Did not comply with federal law requirements for data security and protection; and,
  - d. Otherwise deceived and mislead.
85. As a proximate and direct result of this unlawful and deceptive trade practice, the members of the DC Class were deceived in their purchase of products and services from Defendant in that the DC Class believed Defendant would comply with its own stated privacy policy.
86. As a result of this unfair and deceptive trade practice, the DC Class has been injured and seeks the following on behalf of the general public and members of the class:
- a. Relief to restore to the consumer money which was acquired by means of the unlawful trade practice in the District of Columbia;
  - a. Punitive damages;
  - b. \$1500 per violation or treble damages, whichever is greater;
  - c. Reasonable Attorneys' fees; and,
  - d. All other statutory relief the court determines proper under D.C. Code § 28-3905(k)(1).
87. **WHEREFORE**, Plaintiff Rodd Santomauro on behalf of himself as an individual and on behalf of the general public and the DC Class, make this Complaint for all damages requested above including injunctive relief and all other monetary damages allowed by law believed to be in excess of the jurisdictional amount.

**VIOLATION OF THE DC DATA BREACH NOTIFICATION STATUTE**  
**Count IV**

88. Each of the preceding paragraphs is incorporated by reference herein.
89. The District of Columbia Data Breach Notification Statute (D.C. Code, Loc. Bus. Aff. § 28-3851, *et seq.*) defines “personal information” as “An individual’s first name or first initial and last name, or phone number, or address, and any one or more of the following

data elements: (ii) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.” D.C. Code § 28-3851(3).

90. Defendant was required to notify Rodd Santomauro and the DC Class in the “most expedient time possible” and without unreasonable delay. Defendant was further required to notify all Consumer Reporting Agencies without unreasonable delay of the breach of information of the DC Class.

91. Defendant failed to provide notice of the data breach to Mr. Santomauro and the DC Class in the most expedient time possible and also failed to provide notice of the breach to all required Consumer Reporting Agencies without unreasonable delay.

92. Mr. Santomauro and the DC Class have suffered actual damages in that they and members of the DC Class have purchased and will need to continue to purchase credit monitoring and identity theft protection for life.

93. Mr. Santomauro brings this cause of action on behalf of himself individually and the DC Class seeking all actual damages, costs of the action and reasonable attorneys' fees.

94. **WHEREFORE**, Plaintiff Rodd Santomauro on behalf of himself as an individual and on behalf of the general public and the DC Class, make this Complaint for all damages requested above including injunctive relief and all other monetary damages allowed by law believed to be in excess of the jurisdictional amount.

**VIOLATION OF THE MARYLAND CONSUMER PROTECTION ACT**  
**Count V**

95. Each of the preceding paragraphs is incorporated by reference herein.

96. Defendant produced a privacy policy which informed Brenda Birkett and the Maryland Class that Defendant would protect their PII with industry standard safeguards.

97. However, Defendant violated their privacy policy and committed an unfair and unlawful trade practice in that the privacy policy:

- a. Contained misleading statements that had the capacity and tendency to mislead the Plaintiffs to believe that the personal information which Defendant had in its possession and control would be safeguarded on Defendant's servers.
- b. Stated a material fact that tended to deceive the Maryland Class to believe that their personal information would be protected while in transit and at rest on Defendant's servers.

98. Further, the State of Maryland defines "Personal information" as "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: **(i)** A Social Security number; **(ii)** A driver's license number; or **(iii)** A financial account number...." Md. Commercial Law Code Ann. § 14-3501.

99. A data breach occurred because Equifax permitted unauthorized access to individuals' names, credit card numbers, birth dates, social security numbers, and the Class Members' PII.

100. Defendant was required to notify Plaintiff and the members of the Maryland Class of the security breach as soon as was reasonably practicable after it was discovered.

101. Defendant was further required to send a notification letter which provided the following information:

- (1)** To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person,

including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained;

(3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and

(4) (i) The toll-free telephone numbers, addresses, and Web site addresses for:

- 1. The Federal Trade Commission; and
- 2. The Office of the Attorney General; and

(ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft. Md. Commercial Law Code Ann. § 14-3504.

102. Defendant failed to provide a proper notification in that they, collectively and individually, failed to provide toll free numbers for the major consumer reporting agencies or toll free numbers, addresses, and website addresses for the Federal Trade Commission and the Office of the Attorney General, and to inform the individuals that information can be obtained from these sources about steps that can be taken to avoid identity theft.

103. Defendant committed an unlawful and deceptive trade practice in failing to comply with Maryland Comm. Law Code Ann. § 14-3504, *et seq.*

104. As a proximate and direct result of this failure to comply with Md. Comm. Law Code Ann. § 14-3504, Plaintiff Brenda Birkett and the Maryland Class suffered actual damages in that they were delayed in obtaining timely credit protection and identity theft monitoring and suffered mental and emotional pain and suffering.

105. Plaintiff seeks for herself and the Maryland Class all damages allowable by law for these unlawful and deceptive trade practices including compensatory damages for economic and non-economic harm, and attorneys' fees.

106. **WHEREFORE**, Plaintiff Brenda Birkett on behalf of herself as an individual and on behalf of the Maryland Class, makes this Complaint for all damages requested above including all monetary damages including attorneys' fees as allowed by law and believed to be in excess of the jurisdictional amount.

**VIOLATION OF THE WEST VIRGINIA CONSUMER CREDIT & PROTECTION ACT**  
**Count VI**

107. Each of the preceding paragraphs is incorporated by reference herein.

108. Defendant committed an unlawful trade practice by failing to offer services consistent with its own privacy policy in that Defendant failed to protect Plaintiff Debra Lee's and the West Virginia Class' personal information. This failure is an unlawful trade practice in that it:

- a. Misrepresented the benefits of the services provided by Defendant;
- b. Used deception, fraud and misrepresentation by representing that Plaintiff Debra Lee's and the West Virginia Class' personal information would be protected on Defendant's servers; and,
- c. Otherwise misleading conduct as described herein.

109. As a proximate and direct result of this failure to comply with W.VA. Code § 46A-6-104, Plaintiff Debra Lee and the West Virginia Class suffered actual damages in that they were not given the benefit of the services for which they bargained and ultimately their PII, Sensitive Information was subject to a data breach that encryption and property security measures would have prevented.

110. Plaintiff seeks for the West Virginia Class all damages allowable by law for these unlawful and deceptive trade practices including actual damages, statutory damages, and attorneys' fees and court costs.

111. **WHEREFORE**, Plaintiff Debra Lee, on behalf of herself and the West Virginia Class, make this Complaint for all damages requested above including all monetary damages including attorneys' fees as allowed by law and believed to be in excess of the jurisdictional amount.

**COMMON LAW INVASION OF PRIVACY**  
**Count VII**

112. Each of the preceding paragraphs is incorporated by reference herein.

113. The Plaintiffs have an expectation of privacy to be free from disclosure of their PII and Sensitive Information.

114. The acts of the Defendant in engaging in misleading and negligent protection of PII exposed the Plaintiffs for life and invaded the Plaintiffs' homes and damaged and harmed the Plaintiffs' right of privacy.

115. As a result of the Defendant's actions, the Plaintiffs suffered emotional distress.

116. As a result of the Defendant's actions, Plaintiffs have been annoyed, inconvenienced, harassed, bothered, upset, angered, harangued and otherwise were caused indignation and distress.

117. **WHEREFORE**, Plaintiffs on behalf of themselves as individuals and on behalf of The Class, make this Complaint for all damages allowable by law including all monetary damages including attorneys' fees and punitive damages as allowed by law and believed to be in excess of the jurisdictional amount.

**NEGLIGENCE PER SE**  
**Count VIII**

118. Each of the preceding paragraphs is incorporated by reference herein.
119. Defendant owed the Plaintiffs a duty of care in protecting the confidentiality of the personal and private information of the Plaintiffs.
120. Defendant came into possession of Plaintiffs' PII and Sensitive Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.
121. Defendant further had a duty to comply with applicable state and federal laws which were implemented to protect the Plaintiffs and members of The Class.
122. Defendant failed to comply with the duties imposed upon them by applicable federal laws in protecting Plaintiffs, The Class and the Subclasses by:
- a. Failing to provide reasonable and timely notification of the data breach including by failing to comply with the DC Data Breach Notification statute and the DC Consumer Protection and Procedures Act;
  - b. Failing to comply with the Maryland Consumer Protection Act and the Maryland Data Breach Notification Act (Maryland Comm. Law Code Ann. § 14-3504, *et seq.*); and
  - c. Failing to comply with the West Virginia Consumer Credit and Protection Act.
123. As a direct and proximate result of the Defendant's negligence, the Plaintiffs have suffered damages, including pain and suffering and past and future economic loss.
124. **WHEREFORE**, Plaintiffs demand judgment against Defendant for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together

with interest from the date of the incident and the costs of the proceeding, including attorneys' fees.

**UNJUST ENRICHMENT**  
**Count IX**

125. Each of the preceding paragraphs is incorporated by reference herein.
126. Defendant received payment from Plaintiffs to perform services that included protecting Plaintiffs' Sensitive Information.
127. Defendant did not protect Plaintiffs' Sensitive information, but retained Plaintiffs' payments.
128. Defendant has knowledge of said benefit.
129. Defendant has been unjustly enriched and it would be inequitable for Defendant to retain Plaintiffs' payments.
130. As a result, Plaintiffs have been proximately harmed and/or injured.
131. **WHEREFORE**, Plaintiffs individually and on behalf of the members of The Class demand judgment against Defendant for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

**BREACH OF THE DUTY OF CONFIDENTIALITY**  
**Count X**

132. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.
133. The Defendant owed the Plaintiffs and members of The Class a duty of confidentiality pursuant to its fiduciary relationship with the Plaintiffs and members of The Class as a credit bureau.



134. Included in this duty owed by the Defendant is one of undivided secrecy and loyalty to the Plaintiffs, and this duty is critical to encourage the free exchange of information between individuals and credit bureaus.

135. The minimum standard of care imposed on the Defendant in maintaining the confidentiality of the Plaintiffs' Sensitive Information is expressed in multiple statutes, regulations, and judicial decisions.

136. The Defendant breached its individual and collective duty to the Plaintiffs and members of The Class through the unauthorized disclosure, breach, and/or publication of their personal and private information, and thus violated the Plaintiffs' right to have this information and their information kept confidential.

137. Indeed, such a violation breaches the trust that represents the core of the fiduciary relationship between the Plaintiffs and Defendant.

138. As a direct and proximate result of the Defendant's breach of the duty of confidentiality, the Plaintiffs and members of The Class have suffered damages and breach of the confidential information.

139. **WHEREFORE**, Plaintiffs demand judgment against Defendant for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorneys' fees.

#### **PRAYER FOR RELIEF**

140. **WHEREFORE** Plaintiffs seek individually and on behalf of all others similarly situated, members of The Class, The DC Class, The Maryland Class and the West Virginia Class, all damages allowable by law, including compensatory damages, statutory

damages, punitive damages, attorneys' fees, and costs in excess of \$5 million (\$5,000,000.00) and further seek all injunctive relief allowed by law. The Plaintiffs, individually and on behalf of The Class, further pray for the following relief:

- A. That the Court certify The Class and appoint the Plaintiffs as class representative and The Giatras Law Firm, PLLC as Class counsel.
- B. That the Court enter judgment against Equifax for all damages set forth above, as well as for costs, attorney fees, statutory damages adjusted for inflation, and further relief as the Court deems appropriate.
- C. Compensatory damages for the Plaintiffs general and special damages set forth above;
- D. An award for the Plaintiff's undue and unreasonable harassment, oppression, abuse, aggravation, annoyance, and inconvenience damages;
- E. All statutory damages adjusted for inflation provided for as described above;
- F. Punitive damages for the willful, wanton, oppressive, malicious and/or reckless conduct of the Defendant;
- G. Such other relief as the Court deems equitable and just.

Date: September 8, 2017

Respectfully submitted,

THE GIATRAS LAW FIRM, PLLC

/s/ Troy N. Giatras  
Troy N. Giatras Esq., Bar No. 429086  
118 Capitol Street, Suite 400  
Charleston, WV 25301  
[troy@thewvlawfirm.com](mailto:troy@thewvlawfirm.com)  
(304) 343-2900 (Tel.)  
(304) 343-2942 (Fax)

**DEMAND FOR JURY TRIAL**

*COMES NOW* Plaintiffs, by and through undersigned counsel, and pursuant to Rule 38 of the Federal Rules of Civil Procedure, hereby demands trial by jury of all issues in this matter.

Respectfully submitted,

THE GIATRAS LAW FIRM, PLLC

/s/ Troy N. Giatras  
Troy N. Giatras Esq., Bar No. 429086  
*Counsel for Plaintiffs, The Class and all  
Subclasses*