IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

John WASHBURN, Avery ASH, and Cassandra POWERS, James FINDLAY, AmySue TAYLOR, and Evelyn GUALANDI, on behalf of themselves and all others similarly situated, **Plaintiffs,** **v.** **EQUIFAX, INC.,** **Defendant.**	**Case No.** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

I. INTRODUCTION

1. Plaintiffs John Washburn, Avery Ash, Cassandra Powers, James Findlay, AmySue Taylor, and Evelyn Gualandi, on behalf of themselves and all others similarly situated, bring this action against Equifax, to recover monetary damages, injunctive relief, and other remedies for violations of state statutes and the common law.

II. NATURE OF THE ACTION

2. This action arises out of the massive failure by Equifax, a leading credit-reporting company, to safeguard some of the most sensitive financial and personal information of over 143 million individuals across the U.S., including Plaintiffs.

3. On September 7, 2017, Equifax announced that a giant cybersecurity data breach had occurred in its data systems from mid-May through July 2017. This hack allowed criminals to access names, Social Security numbers, birth dates, addresses, and driver's license numbers, for millions of individuals. In addition, Equifax reported that the hackers gained access to approximately 209,000 customers' credit card numbers, and had gained access to financial dispute documents containing personal identifying information for approximately 182,000 U.S. customers.

4. Equifax's wrongful conduct includes, upon information and belief, failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' financial and personal data, and failing to provide timely and adequate notice of the data breach. Equifax admitted that it discovered the unauthorized access on July 29, 2017, yet did not inform the public of this breach until more than a month later, on September 7, 2017.

5. Equifax's action and failure to act when required has caused Plaintiffs and millions of others to suffer harm and/or face the significant risk of future harm, including but not limited to:

a. unauthorized charges on their debit and credit card accounts;

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. 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;

e. costs associated with time spent and the loss of productivity 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, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax data breach;

f. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet card black market;

g. damages to and diminution in value of their personal and financial information entrusted to Equifax with the mutual understanding

that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

h. continued risk to their financial and personal information, which remains in Equifax's possession and is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data in its possession.

6. Plaintiffs, individually and on behalf of the other Class members, seek to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated consumers whose account and/or personally identifying information was stolen as a result of the Equifax data breach. Plaintiffs assert claims for themselves and on behalf of a nationwide class of consumers for Equifax's violation of the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.*, as well as for (1) negligence, (2) bailment, and (3) unjust enrichment and on behalf of a subclass of District of Columbia consumers under (4) the District of Columbia Consumer Protection Procedures Act (DCCPPA), D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), *et seq.*, and (5) the District of Columbia data breach statute, D.C. Code § 28-3851 *et seq.*

7. Plaintiffs seek to recover, for themselves and the other Class members, actual and statutory damages, injunctive relief to prevent a recurrence of

the data breach, restitution, disgorgement, and costs and reasonable attorneys' fees.

III. PARTIES

A. Plaintiffs.

8. John Washburn is a resident of the DeKalb County, Georgia. Upon information and belief, Mr. Washburn's Social Security number and other personally identifying information were exposed by Equifax. Mr. Washburn first learned of this breach from a news source. After speaking with a friend about the breach, Mr. Washburn went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Washburn's information was exposed as a result of Equifax's massive data breach.

9. Avery Ash is a resident of the District of Columbia. Upon information and belief, Mr. Ash's Social Security number and other personally identifying information were exposed by Equifax. Mr. Ash first learned of this breach from a news story posted on the internet. Concerned his information may have been comprised, Mr. Ash went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Ash's information was exposed as a result of Equifax's massive data breach.

10. Cassandra Powers is a resident of the District of Columbia. Upon information and belief, Ms. Powers's Social Security number and other personally identifying information were exposed by Equifax. Ms. Powers first learned of this breach from a friend at a softball game. Concerned her information may have been comprised, Ms. Powers went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Powers's information was in fact exposed as a result of Equifax's massive data breach.

11. James Findlay is a resident of the State of Illinois. Upon information and belief, Mr. Findlay's Social Security number and other personally identifying information were exposed by Equifax. Mr. Findlay first learned of this breach from a news story posted on the Internet. Concerned that his information may have been comprised, Mr. Findlay went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if his information was exposed. The response from the website indicated that Mr. Findlay's information was exposed as a result of Equifax's massive data breach.

12. AmySue Taylor is a resident of the State of Ohio. Upon information and belief, Ms. Taylor's Social Security number and other personally identifying information were exposed by Equifax. Ms. Taylor first learned of this breach from

a news story posted on the Internet. Concerned that her information may have been comprised, Ms. Taylor went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Taylor's information was exposed as a result of Equifax's massive data breach.

13. Evelyn Gualandi is a resident of the State of Indiana. Upon information and belief, Ms. Gualandi's Social Security number and other personally identifying information were exposed by Equifax. Ms. Gualandi first learned of this breach from a news story posted on the Internet. Concerned that her information may have been comprised, Ms. Gualandi went to Equifax's emergency response website, trustedidpremier.com, and followed the prompts to determine if her information was exposed. The response from the website indicated that Ms. Gualandi's information was exposed as a result of Equifax's massive data breach.

B. Defendant.

14. Equifax is a Georgia corporation, with its principal place of business in Atlanta, Georgia. Equifax is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Georgia, which is located in Fulton County, Georgia.

IV. JURISDICTION AND VENUE

15. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiffs and Class members assert that Equifax violated the FCRA, and therefore Plaintiffs' and Class members' claim arises under the laws of the United States.

16. In addition, this Court has subject-matter jurisdiction the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action, including claims asserted on behalf of a nationwide class, filed under Rule 23 of the Federal Rules of Civil Procedure; there are hundreds of thousands, and likely millions, of proposed Class members; the aggregate amount in controversy exceeds the jurisdictional amount or $5,000,000.00; and Equifax is a citizen of a State different from that of Plaintiffs. This Court also has subject-matter jurisdiction over Plaintiffs' and Class members' claims pursuant to 28 U.S.C. § 1367(a).

17. Venue is proper in this District under 28 U.S.C. § 1391 (a)–(d) because, *inter alia*, substantial parts of the events or omissions giving rise to the claim occurred in the District and/or a substantial part of property that is the subject of the action is situated in the District. A substantial part of Plaintiffs' personal and financial information and activities that Equifax collected, obtained, maintained, and allowed to be accessed without authorization during the data

breach, occurred in or was found in the District. And, a significant part of the risk of harm that Plaintiffs now face through Equifax's wrongful conduct is present in this District. Venue is also proper in the Atlanta Division because Equifax is located here.

V. FACTS

A. Equifax's Business – Collecting Sensitive Financial and Personal Information on Millions of Individuals

18. Equifax describes itself as "a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions. The company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."

19. In its SEC filings, Equifax states that "[w]e collect, organize and manage various types of financial, demographic, employment and marketing information. Our services enable businesses to make credit and service decisions, manage their portfolio risk, automate or outsource certain human resources, employment tax and payroll-related business processes, and develop marketing

strategies concerning consumers and commercial enterprises. We serve customers across a wide range of industries, including the financial services, mortgage, retail, telecommunications, utilities, automotive, brokerage, healthcare and insurance industries, as well as government agencies. We also enable consumers to manage and protect their financial health through a portfolio of products offered directly to consumers. We also provide information, technology and services to support debt collections and recovery management."

20. Equifax is publicly traded on the New York Stock Exchange (ticker symbol EFX). In 2016 it generated revenues of $3.144 billion.

21. Equifax is one of three nationwide credit-reporting companies that track and rate the financial history of U.S. consumers. Equifax is supplied with data about loans, loan payments and credit cards, as well as information on everything from credit limits and terms to employment history, from child support payments to missed rent and utilities payments. All of this highly sensitive information then is factored into the credit reports that Equifax maintains and provides to financial companies, employers, and other entities who use those scores to make decisions about individuals in a range of areas.

22. In addition, Equifax provides a variety of services to consumers themselves, such as period credit reports and credit scores, credit monitoring, and

even – ironically – identity theft protection.

23. Of course, these services, too, involve consumers providing Equifax with sensitive financial and personal information as part of the consumers paying for, and Equifax providing, such services.

24. Perhaps no other corporations in the U.S. maintain as much sensitive personal and financial information about consumers as do Equifax and the other two credit-reporting companies.

25. Understandably, then, it is of paramount importance for a company such as Equifax to protect and secure from intrusion and hacking the enormous amount of sensitive information about individuals that it maintains and uses for its business purposes.

B. Equifax Experiences Earlier Data Breaches, But Fails To Take Steps To Secure Its Data Systems From Future Attacks

26. Far from being unforeseeable, this latest breach appears similar to two intrusions that Equifax experienced recently, one in 2016 and one in early 2017.

27. In those earlier hacking incidents, cybercriminals exploited a vulnerability in an Equifax website to steal W-2 tax data.

28. Those incidents served to put Equifax on notice of a startling reality: it had not taken the appropriate measures to secure its huge volume of sensitive information about consumers' intimate financial and personal details.

29. A responsible company would have taken swift and decisive action to remedy its cybersecurity shortcomings. But upon information and belief, Equifax failed to undertake such measures.

C. Equifax Experiences A Massive Data Breach, Which It Hides From The Public For More Than A Month

30. Between mid-May through July 2017, cyber criminals exploited a vulnerability in a U.S. website application to gain access to Equifax data systems.

31. Those data systems included names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers and other personally identifying information for up to 143 million U.S. customers, or roughly 44% of the U.S. population.

32. Similar personal identifying information was also accessed for an undisclosed number of U.K. and Canadian customers.

33. According to a company press release, Equifax identified the intrusion on July 29, 2017.

34. However, the company waited until September 7, 2017 to announce the intrusion to the public. In the interim, while the breach was still unknown to the public, three senior executives, including chief financial officer, John Gamble, President of U.S. information solutions, Joseph Loughran, and president of workforce solutions Rodolfo Ploder sold shares worth almost $1.8 million in total,

according to a Bloomberg report. The same report stated that the shares were not listed as part of a 10b5-1 scheduled trading plan.

35. The types of information that were compromised jeopardize consumers' bank accounts, medical records, and credit accounts. According to Avivah Litam, a fraud analyst at leading information technology consulting and research firm, Gartner, Inc., "On a scale of 1-to 10 in terms of risk to consumers, this a 10."

36. Senator Mark Warner of Virginia stated "It is no exaggeration to suggest that a breach such as this — exposing highly sensitive personal and financial information central for identity management and access to credit — represents a real threat to the economic security of Americans."

37. Equifax's Chairman and Chief Executive Officer, Richard F. Smith, gave the following statement:

> "This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes. We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations."

38. This most recent and more damaging intrusion is evidence that Equifax has persisted in its failure to take appropriate measures to secure itself against known or foreseeable vulnerabilities. Thus, despite its professed leadership in "managing and protecting" data, Equifax has known, or should have known, that the picture it presents to the public does not match up with its actual cybersecurity protections – or lack thereof.

39. Equifax failed to disclose to the public, including Consumer Plaintiffs and members of the Class, that its computer systems and security practices were inadequate to safeguard customers' financial account and personal identifying information against theft.

40. Equifax failed to disclose and provide timely and accurate notice of the data breach to the public, including Plaintiffs and the other Class members.

D. Equifax's Notice To The Public Was Insufficient and Deceptive.

41. Equifax published a press release on September 7, 2017 on its website which linked to a page where consumers could provide their last name and the last 6 digits of their Social Security number to "See if [their] personal information was potentially impacted." This link was circulated by countless online media companies, blogs and social networks. However, after completing this process many people simply received a notice to enroll in "TrustedId Premier," an Equifax

credit monitoring service. Contrary to the solicitation by Equifax, the application did not indicate whether one's information had been potentially impacted. This is deceptive and insufficient notice.

42. Compounding the insufficiency of the notice, Equifax was bizarrely unprepared to handle the traffic its website and phone lines would receive after announcing the breach of more than 143,000,000 people personal financial information. Equifax's website and phone lines crashed repeatedly, leaving panicked consumers unable to determine whether their information was compromised. Additionally, those consumers who did manage to get through to check whether they were affected were left confused when an apparent bug in the website coding gave them different results as to whether their information was compromised based on what browser they used. This lack of preparation for such an immensely foreseeable demand is inexplicable, and inexcusable, for an organization that holds itself out as an elite information technology company.

E. Plaintiffs and the Other Class Members Now Face A Significant Risk of Harm From Equifax Allowing Their Sensitive Personal and Financial Information To Be Hacked.

43. Equifax's conduct and failures now have placed Plaintiffs and the other Class members at significant risk of harm.

44. Equifax's data breach revealed to identity thieves highly valuable

personal and financial information of consumers, including Plaintiffs and the other Class members.

45. The FTC warns consumers to pay particular attention to how they keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data.

46. 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."

47. Personal and financial information such as that stolen in the Equifax data breach is highly coveted by, and a frequent target of, hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts. The thieves use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards. Additionally, the thieves could reproduce stolen debit cards and use them to withdraw cash from ATMs.

48. Identity theft occurs when someone uses another's personal and financial information such as that person's name, address, credit card number,

credit card expiration dates, and other information, without permission, to commit fraud or other crimes.

49. Identity thieves can use personal information such as that pertaining to Plaintiffs and the other Class members, which Equifax failed to keep secure, to perpetuate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of crimes 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.

50. In addition, identity thieves may get medical services using consumers' lost information or commit any number of other frauds, such as obtaining a job, procuring housing or even giving false information to police during an arrest.

51. A cyber black market exists in which criminals openly post and sell stolen credit card numbers, Social Security numbers and other personal information on a number of Internet websites.

52. The personal and financial information that Equifax failed to adequately protect and that was stolen in the Equifax data breach, including Plaintiffs' and the other Class members' identifying information, allow identity

thieves to use victims' personal data 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.

53. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

54. In sum, the ramifications of Equifax's failure to keep Plaintiffs' and the other Class members' personal and financial information secure are severe, and likely to be lasting.

VI. CLASS ALLEGATIONS

55. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring their claims that Equifax violated the FCRA as well as for common law negligence, bailment, and unjust enrichment, on behalf of themselves and the following national class:

NATIONAL CLASS

> All residents of the United States whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017.

56. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs bring their claims that Equifax is liable for statutory violations of the District of Columbia Consumer Protection Act, D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), *et seq*.,

and the District of Columbia data breach statute, D.C. Code § 28-3852(a), on behalf of themselves and the following District of Columbia Subclass:

DISTRICT OF COLUMBIA SUBCLASS

All residents of the District of Columbia whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017.

57. Excluded from the foregoing Class and Subclass are Equifax, its officers and directors, as well as the judge to whom this case is assigned.

58. The Class and Subclass consist of millions of individuals, making joinder impractical, in satisfaction of FRCP 23(a)(1). The exact size of the Class and Subclasses and the identities of the individual members thereof are ascertainable through Equifax's records, including but not limited to its billing and collection records.

59. The claims of Plaintiffs are typical of the claims of the other Class and Subclass members. The claims of the Plaintiffs and the members of the Class and Subclass are based on the same legal theories and arise from the same unlawful and willful conduct, resulting in the same injury to the Plaintiffs and their respective classes.

60. The respective classes have a well-defined community of interest. Equifax has acted and failed to act on grounds generally applicable to the Plaintiffs

and the Class and Subclasses, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the respective classes.

61. There are many questions of law and fact common to the claims of Plaintiffs and the other Class and Subclass members, and those questions predominate over any questions that may affect only individual class members. Common questions of fact and law affecting members of the Class and Subclasses that predominate over any individualized questions include, but are not limited to, the following:

a. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

b. Whether Equifax failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Equifax failed to take available steps to prevent and stop the breach from ever happening;

d. Whether Equifax failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' financial and personal data;

e. Whether Equifax failed to provide timely and adequate notice of the data breach;

f. Whether Equifax owed a duty to Plaintiffs and the other Class and Subclass members to protect their personal and financial information and to provide timely and accurate notice of the data breach to Plaintiffs and the other Class and Subclass members;

g. Whether Equifax breached its duties to protect the personal and financial information of Plaintiffs and the other Class and Subclass members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiffs and the other Class and Subclass members of the data breach;

h. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of millions of consumers' personal and financial information;

i. Whether Equifax's conduct amounted to violations of the FCRA, the District of Columbia Consumer Protection Act, and the District of Columbia data breach statute;

j. Whether Equifax's conduct renders it liable for negligence, bailment, and unjust enrichment;

k. Whether, as a result of Equifax's conduct, Plaintiffs and the other

Class and Subclass members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

l. Whether, as a result of Equifax's conduct, Plaintiffs and the other Class and Subclass members are entitled to injunctive, equitable and/or other relief, and, if so, the nature of such relief.

62. Absent a class action, most of the Class and Subclass members would find the cost of litigating their claims to be prohibitive and will have no effective remedy. The class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

63. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual Class and Subclass members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

64. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Equifax has acted or has refused to act on grounds generally

applicable to the Class and Subclass, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class and Subclass as a whole.

65. Plaintiffs will fairly and adequately represent and protect the interests of the Class and Subclass. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other Class and Subclass members, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interests adverse to those of the other members of the Class and Subclass.

VII. CAUSES OF ACTION

COUNT 1: VIOLATION OF FAIR CREDIT REPORTING ACT (FCRA), 15 U.S.C. § 1681 *et seq.*,

Asserted by the National Class against Equifax

66. Plaintiffs repeat paragraphs 1 through 65, above, as if fully alleged herein.

67. Plaintiffs and Class members are each a "consumer" as defined in 15 U.S.C. § 1681a(c).

68. Equifax is a "consumer reporting agency" and a "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" as

defined in 15 U.S.C. § 1681a(f) and (p), respectively.

69. Equifax compiled and maintained a "consumer report" on each Plaintiff and Class member, as defined in 15 U.S.C. § 1681a(d): a "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 credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 1681b of this title."

70. Under FCRA, Equifax had an obligation to protect from disclosure Plaintiffs' and the other Class members' consumer reports under the circumstances alleged herein. Section 1681b prohibits a consumer reporting agency from disclosing a consumer report except as permitted under the statute.

71. Section 1681e of FCRA requires every consumer reporting agency to maintain reasonable procedures designed to avoid violations of FCRA and to limit the furnishing of consumer reports to the purposes permitted under the statute.

72. As a direct and proximate result of Equifax's actions and failures to act described herein, including, without limitation, its failure to take adequate and

reasonable measures to ensure its data systems were protected, and failure to take appropriate steps to prevent and stop the data breach from ever happening, Equifax allowed unauthorized criminal computer hackers to obtain consumer reports of Plaintiffs and the other Class members.

73. Equifax's disclosure of consumer reports under these circumstances was not permitted by, and thus in violation of, Sections 1681b and e of FCRA.

74. As a direct and proximate result of Equifax's actions and failures to act described herein, including, without limitation, its failure to take adequate and reasonable measures to ensure its data systems were protected, and failure to take appropriate steps to prevent and stop the data breach from ever happening, Equifax caused Plaintiffs and the other Class members to suffer harm and/or face the significant risk of harm in the future, including, among other things, the harm and threat of harm described above.

75. Under Section 1681o of FCRA, Equifax is liable to Plaintiffs and the other Class members for negligently failing to comply with the requirements not to disclose consumer reports, and to take measures designed to avoid the unauthorized disclosure of consumer reports. Equifax therefore is liable to Plaintiffs and the other Class members for any actual damages they sustain as a result of Equifax's failure, as well as costs and reasonable attorneys' fees, in

amounts to be proven at trial.

76. In addition, Equifax's failure to comply with the foregoing requirements was willful because, upon information and belief, Equifax knew or should have known, but recklessly disregarded, that its cybersecurity measures were not adequate and reasonable to protect consumers' sensitive financial and personal data from security breaches.

77. Therefore, Equifax is liable to Plaintiffs and the other Class members in an amount equal to actual damages, or damages of not less than $100 and not more than $1,000 for each Plaintiff and other Class member, as well as punitive damages as the Court may allow.

COUNT 2: NEGLIGENCE

Asserted by the Nationwide Class against Equifax

78. Plaintiffs repeat paragraphs 1 through 65, above, as if fully alleged herein.

79. Equifax owed a duty to Plaintiffs and the other Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's

security systems to ensure that Plaintiffs' and the other Class members' personal and financial information in Equifax's possession was adequately secured and protected. Equifax further owed a duty to Plaintiffs and the other Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

80. Equifax owed a duty to Plaintiffs and the other Class members to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and the other Class members about whom Equifax collected, maintained, and used such information.

81. Equifax owed a duty of care to Plaintiffs and the other Class members because they were foreseeable and probable victims of any inadequate security practices. Equifax solicited, gathered, and stored the personal and financial data provided by Plaintiffs and the other Class members to facilitate its provision of credit score and other financial information to customers. Equifax knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempted to access this valuable data without authorization.

82. Equifax knew that a breach of its systems would cause damages to Plaintiffs and the other Class members and Equifax had a duty to adequately protect such sensitive financial and personal information.

83. Equifax owed a duty to timely and accurately disclose to Plaintiffs and the other Class members that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and the other Class members could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

84. Plaintiffs and the other Class members entrusted Equifax with their personal and financial information, on the premise and with the understanding that Equifax would safeguard their information, and Equifax was in a position to protect against the harm suffered by Plaintiffs and the other Class members as a result of the Equifax data breach.

85. Equifax knew, or should have known, of the risks inherent in

collecting and storing the personal and financial information of Plaintiffs and the other Class members and of the critical importance of providing adequate security of that information.

86. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and the other Class members. Equifax's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein. Equifax's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the personal and financial information of Plaintiffs and the other Class members.

87. Equifax breached the duties it owed to Plaintiffs and the other Class members by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Plaintiffs and the other Class members.

88. Equifax breached the duties it owed to Plaintiffs and the other Class members by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

89. Equifax breached the duties it owed to Plaintiffs and the other Class members by failing to properly maintain their sensitive personal and financial information. Given the risk involved and the amount of data at issue, Equifax's

breach of its duties was entirely unreasonable.

90. Equifax breached its duties to timely and accurately disclose that Plaintiffs' and the other Class members' personal and financial information in Equifax's possession had been or was reasonably believed to have been, stolen or compromised.

91. Equifax's failure to comply with its legal obligations and with industry standards and regulations, and the delay between the date of intrusion and the date Equifax disclosed the data breach, further evidence Equifax's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' personal and financial information in Equifax's possession.

92. Equifax knew that Plaintiffs and the other Class members were foreseeable victims of a data breach of its systems because of laws and statutes that require Equifax to reasonably safeguard sensitive payment information, including the District of Columbia data breach statute, D.C. Code § 28-3851, *et seq.*

93. But for Equifax's wrongful and negligent breach of its duties owed to Plaintiffs and the other Class members, their personal and financial information would not have been compromised.

94. The injury and harm suffered by Plaintiffs and members of the Class

as set forth above was the reasonably foreseeable result of Equifax's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' personal and financial information within Equifax's possession. Equifax knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Plaintiffs' and the other Class members' personal and financial information were inadequate and vulnerable to being breached by hackers.

95. Plaintiffs and the other Class members suffered injuries and losses described herein as a direct and proximate result of Equifax's conduct resulting in the data breach, including Equifax's lack of adequate reasonable and industry standard security measures. Had Equifax implemented such adequate and reasonable security measures, Plaintiffs and the other Class members would not have suffered the injuries alleged, as the Equifax data breach would likely have not occurred.

96. As a direct and proximate result of Equifax's negligent conduct, Plaintiffs and the other Class members have suffered injury and the significant risk of harm in the future, and are entitled to damages in an amount to be proven at trial.

COUNT 3: BAILMENT

Asserted by the Nationwide Class against Equifax

97. Plaintiffs repeat paragraphs 1 through 65, above, as if fully alleged herein.

98. Plaintiffs and the other Class members provided, or authorized disclosure of, their personal and financial information to Equifax for the exclusive purpose of Equifax preparing consumer reports, credit monitoring and identity theft protection, and similar services and legitimate business uses.

99. In allowing their personal and financial information to be made available to Equifax, Plaintiffs and the other Class members intended and understood that Equifax would adequately safeguard their personal and financial information.

100. Equifax accepted possession of Plaintiffs' and the other Class members' personal and financial information for the purpose of making available to Plaintiffs and the other Class members Equifax's services for their benefit.

101. By accepting possession of Plaintiffs' and the other Class members' personal and financial information, Equifax understood that Plaintiffs and the other Class members expected Equifax to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the

mutual benefit of the parties. During the bailment (or deposit), Equifax owed a duty to Plaintiffs and the other Class members to exercise reasonable care, diligence, and prudence in protecting their personal and financial information.

102. Equifax breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and the other Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and the other Class members' personal and financial information.

103. Equifax further breached its duty to safeguard Plaintiffs' and the other Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the Equifax data breach.

104. As a direct and proximate result of Equifax's breach of its duty, Plaintiffs and the other Class members suffered consequential damages that were reasonably foreseeable to Equifax, including but not limited to the damages set forth above.

105. As a direct and proximate result of Equifax's breach of its duty, the personal and financial information of Plaintiffs and the other Class members entrusted to Equifax during the bailment (or deposit) was damaged and its value

diminished.

COUNT 4: UNJUST ENRICHMENT

Asserted by the Nationwide Class against Equifax

106. Plaintiffs repeat paragraphs 1 through 65, above, as if fully alleged herein.

107. Equifax knowingly received and retained wrongful benefits and funds from Plaintiffs and Subclass members in the form of compiling and using sensitive information of Plaintiffs and the other Class members, and from monies paid by Subclass members who purchased services from Equifax.

108. Equifax appreciates or has knowledge of the benefits conferred directly upon it by Plaintiffs and the other Class members.

109. As a result of Equifax's wrongful conduct as alleged herein, Equifax has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the other Class members.

110. Equifax's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and the other Class members' sensitive personal and financial information, while at the same failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

111. Under the common law doctrine of unjust enrichment, it is inequitable for Equifax to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiffs and the other Class members in an unfair and unconscionable manner. Equifax's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

112. Plaintiffs and the other Class members did not confer these benefits officiously or gratuitously, and it would be inequitable and unjust for Equifax to retain these wrongfully obtained profits.

113. Equifax is therefore liable to Plaintiffs and the other Class members for restitution in the amount of Equifax's wrongfully obtained profits.

COUNT 5: VIOLATION OF DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT, DISTRICT OF COLUMBIA CODE §§ 28-3901-13.

Asserted by the District of Columbia Subclass against Equifax

114. Plaintiffs Avery Ash and Cassandra Powers ("Plaintiffs," for purposes of this Count) repeat paragraphs 1 through 65, above, as if fully alleged herein.

115. Plaintiffs and the other Subclass members are each a "consumer" as defined in Section 28-3901(a)(2) of the DCCPPA.

116. Equifax is a "merchant" as defined in Section 28-3901(a)(3) of the DCCPPA.

117. Equifax engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and the other Subclass members.

118. Equifax is engaged in, and its acts and omissions affect, trade and commerce. Equifax's acts, practices and omissions were done in the course of Equifax's business of marketing, offering for sale and selling goods and services throughout the United States, including in the District of Columbia.

119. Equifax's conduct as alleged in this Complaint, including without limitation, Equifax's failure to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information, Equifax's failure to disclose the material fact that Equifax's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, and Equifax's failure to disclose in a timely and accurate manner to Plaintiffs and the other Subclass members the material fact of the Equifax data security breach.

120. Equifax's conduct constitutes unlawful trade practices, in violation of, *inter alia*, Sections 28-3904(a), (d), (e), and (f) of the DCCPPA.

121. As a direct and proximate result of the unlawful trade practices described herein, Equifax caused Plaintiffs and the other Subclass members harm,

and/or caused them to face a significant risk of future harm.

122. Equifax is therefore liable to Plaintiffs and the other Subclass members under Section 28-3905(k) of the DCCPAA, for trebled actual damages or $1,500 per violation, whichever is greater, as well as punitive damages, and costs and attorneys' fees, in amounts to be proven at trial.

123. In addition, Plaintiffs and the other Subclass members are entitled to injunctive relief prohibiting Equifax from engaging in, or failing to take required actions to avoid, the wrongful conduct described herein.

COUNT 6: VIOLATION OF DISTRICT OF COLUMBIA CODE §§ 28-3851, *et seq.*

Asserted by the District of Columbia Subclass against Equifax

124. Plaintiffs Avery Ash and Cassandra Powers ("Plaintiffs," for purposes of this Count) repeat paragraphs 1 through 65, above, as if fully alleged herein.

125. Section 28-3852(a) of the D.C. Code provides as follows:

> Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine

the scope of the breach and restore the reasonable integrity of the data system.

126. The breach of Equifax's data systems, and the criminal attackers' resultant unauthorized access to Plaintiffs' and the other Subclass members' personal and financial information, constitutes a "breach of the security system" for purposes of Sections 28-3851 and 28-3852.

127. Plaintiffs' and the other Subclass members' names, addresses, Social Security numbers, drivers' license numbers, credit and debit card numbers, financial dispute information, and other similar information maintained by Equifax and accessed during the data breach, constitute personal information under Sections 28-3851 and 28-3852.

128. Equifax unreasonably delayed in informing the public, including Plaintiffs and the other Subclass members, about the breach of security of Plaintiffs' and the other Subclass members' confidential, non-public, and/or sensitive personal information after Equifax knew or should have known that the data breach had occurred. Equifax waited more than a month after it had learned of the data breach to disclose publicly that it occurred, and to make available a means by which Plaintiffs and the other Subclass members could attempt to learn on their own whether or not they had been impacted.

129. Plaintiffs and the other Subclass members suffered harm directly

resulting from Equifax's failure to provide, and delay in providing, timely and accurate notice as required by Sections 28-3851 and 28-3852.

130. Had Equifax provided timely and accurate notice of the data breach, Plaintiffs and the other Subclass members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice.

131. Equifax therefore is liable under Section 28-3853(a) for Plaintiffs' and the other Subclass members' actual damages as well as costs and attorneys' fees, in amounts to be proven at trial.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class and Subclass members, respectfully request that the Court enter judgment in their favor and against Equifax, as follows:

132. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper Class representatives; and appoint Plaintiffs' attorneys as Class Counsel;

133. That the Court grant permanent injunctive relief to prohibit Equifax from continuing to engage in the unlawful acts, omissions, and practices described

herein;

134. That the Court award Plaintiffs and the other Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

135. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Equifax as a result of its unlawful acts, omissions, and practices;

136. That the Court award statutory damages, and punitive or exemplary damages, to the extent permitted by law;

137. That the unlawful acts alleged in this Complaint be adjudged and decreed to be a violation of the unfair and deceptive business acts and practices in violation of the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, *et seq.*; the District of Columbia Consumer Protection Act, D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), *et seq.*; the District of Columbia data breach statute, D.C. Code § 28-3852(a); negligence; bailment; and unjust enrichment;

138. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, including fees and expenses under O.C.G.A. §13-6-11;

139. That the Court award pre- and post-judgment interest at the maximum legal rate; and

140. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: September 8, 2017

Respectfully submitted,

By: */s/ Kenneth S. Canfield*
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree St., NE, Suite 1900
Atlanta, Georgia 30309
Tel: 404-881-8900
kcanfield@dsckd.com

James Pizzirusso (Pro hac to be submitted)
Richard Lewis (Pro hac to be submitted)
HAUSFELD
1700 K St. NW, Suite 650
Washington, D.C. 20006
Tel: 202-540-7200
jpizzirusso@hausfeld.com
rlewis@hausfeld.com

Pat A. Cipollone, P.C. (Pro hac to be submitted)
Robert B. Gilmore (Pro hac to be submitted)
STEIN MITCHELL MUSE CIPOLLONE & BEATO LLP
1100 Connecticut Ave., N.W.
Washington, D.C. 20036
Tel: 202-737-7777
pcipollone@steinmitchell.com
rgilmore@steinmitchell.com

Andrew N. Friedman (Pro hac to be submitted)
Douglas J. McNamara (Pro hac to be submitted)
Sally Handmaker (Pro hac to be submitted)
COHEN MILSTEIN, SELLERS & TOLL PLLC
1100 New York Avenue, NW, Suite 500
Washington, D.C. 20005
Tel: 202-408-4600
afriedman@cohenmilstein.com
dmcnamara@cohenmilstein.com
shandmaker@cohenmilstein.com

Adam J. Levitt (Pro hac to be submitted)
Amy E. Keller (Pro hac to be submitted)
Daniel R. Ferri (Pro hac to be submitted)
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900
alevitt@dlcfirm.com
akeller@dlcfirm.com
dferri@dlcfirm.com

Counsel for Plaintiffs and the Proposed Class and Subclass