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

ANDREW MCDOWELL, JENNIFER PARKER, MORGAN MCCLUNG, CHEVERA BLAKEMORE, COLTON GREGORY, OLIVIA DAVIS, PATRICK DAVIS BARBARA QUEENEN, LILY ZHOU, MAGGIE MCKINNEY, ASHLEY MIRANDA HALL, CHRIS ALLISON, JOE SPELLMAN, CLAIBORNE REED, CHRISTOPHER TAMBURELLO, PAUL FALKENBERG, TOM CRUMLY, WILLIAM MORIARTY, DOUGLAS HAMMEL, AMANDA LOTS, ANN MARIE WALSH, DANIEL WALSH, RONALD PARKER, JOSIE LOU SMITH, LARA KNEBEL, JOE YODER, DESIRAE BROADHEAD, RONALD BROWN, ASHLIE ATKINSON, REBEKAH RHODES, KYLE HANNAH, COURTNEY FINCH, MICHAEL FINCH, HERSCHEL SIGALL, MEREDITH VILLINES, NICHOLAS WATSON, JESSICE WATSON, GREGORY KESDEN, KEITH REISMAN, JASON PIPPIN, ROBIN SMITH, ANTHONY DIMMAGIO, KURT ZENDE, and CAROL BARBER, individually and on behalf of all others similarly situated Plaintiffs, v. EQUIFAX, INC. Defendant	)	Case No.

CLASS ACTION COMPLAINT

Plaintiffs identified below (collectively "Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Equifax, Inc. ("Equifax" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

INTRODUCTION

1. This action arises from a months-long data breach experienced by Equifax during the spring and summer of 2017. Through this breach, hackers were able to exploit "a garden variety website flaw" to obtain a massive amount of the most sensitive personal data available, acquiring the full names, Social Security Numbers, birth dates, addresses and drivers license numbers of over 143 million Americans.[1]

2. Beyond the severity and scope of the pilfered data, the Equifax breach also stands out for the way the company handled the breach once it was discovered. Although Equifax was aware of the breach as early as July, 2017, it did nothing to apprise affected individuals—almost 50% of the U.S. population—until September

[1] https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/

7, 2017. During that time, three Equifax executives were permitted to sell more than $1.8 million worth of stock in the days following the company's discovery of the breach.[2]

3. Noted security researcher Brian Krebs described Equifax's response to the breach as "completely broken at best, and little more than a stalling tactic or sham at worst."[3] Of particular concern, the website the company created to inform people whether they were affected by the breach would provide results seemingly at random: "In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones."

> Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring services we were eligible for were not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.[4]

4. Further, in the course of providing remedial measures to affected

[2] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/
[3] https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/
[4] *Id.*

consumers, Equifax offers a year's worth of credit monitoring services that in turn require the user to agree to binding arbitration, thereby foregoing any legal remedy in the courts for harm caused by Equifax's data breach. Doing so also lowers the cost to Equifax for future credit monitoring services as many victims of the breach, including Plaintiffs, will not succumb to forgoing their legal rights to redress in court.

5. As a result of the staggering array of personal information that has been compromised, Plaintiff and Class members will have to remain vigilant for the rest of their lives to combat potential identity theft arising from the critical (and in some instances, irreplaceable) data that are in the hands of cyber criminals, who may use such data for any purpose, at any point, in perpetuity. Despite all best efforts of Plaintiff and Class Members, or any other third party to scrub these data from the World Wide Web, they are potentially forever recoverable by anyone who wishes to find them.

6. As detailed below, Equifax's acts, practices, and omissions violate the laws of numerous states, and Plaintiffs bring this action on behalf of themselves, a nationwide class, and multiple state subclasses.

THE PARTIES

7. Plaintiff Andrew McDowell is a citizen of the State of Alabama. Upon information and belief, his personal information, including full name, Social

Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

8. Plaintiff Jennifer Parker is a citizen of the State of Alaska. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

9. Plaintiff Morgan McClung is a citizen of the State of Arizona. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

10. Plaintiff Chevera Blakemore is a citizen of the State of Arkansas. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

11. Plaintiff Colton Gregory is a citizen of the State of Arkansas. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

12. Plaintiff Olivia Davis is a citizen of the State of Arkansas. Upon information and belief, her personal information, including full name, Social

Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

13. Plaintiff Patrick Davis is a citizen of the State of Arkansas. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

14. Plaintiff Barbara Queenen is a citizen of the State of California. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

15. Plaintiff Lily Zhou is a citizen of the State of California. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

16. Plaintiff Maggie McKinney is a citizen of the State of California. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

17. Plaintiff Ashley Miranda Hall is a citizen of the State of Colorado. Upon information and belief, her personal information, including full name, Social

Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

18. Plaintiff Chris Allison is a citizen of the State of Colorado. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

19. Plaintiff Joe Spellman is a citizen of the State of Connecticut. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

20. Plaintiff Claiborne Reed is a citizen of the State of Florida. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

21. Plaintiff Christopher Tamburello is a citizen of the State of Florida. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

22. Plaintiff Paul Falkenberg is a citizen of the State of Georgia. Upon information and belief, his personal information, including full name, Social

Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

23. Plaintiff Tom Crumly is a citizen of the State of Hawaii. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

24. Plaintiff William Moriarty is a citizen of the State of Iowa. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

25. Plaintiff Douglas Hammel is a citizen of the State of Louisiana. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

26. Plaintiff Amanda Lotts is a citizen of the State of Maryland. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

27. Plaintiff Ann Marie Walsh is a citizen of the Commonwealth of Massachusetts. Upon information and belief, her personal information, including

full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

28. Plaintiff Daniel Walsh is a citizen of the Commonwealth of Massachusetts. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

29. Plaintiff Ronald Parker is a citizen of the State of Michigan. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

30. Plaintiff Josie Lou Smith is a citizen of the State of Mississippi. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

31. Plaintiff Lara Knebel is a citizen of the State of Missouri. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

32. Plaintiff Joe Yoder is a citizen of the State of Missouri. Upon information and belief, his personal information, including full name, Social

Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

33. Plaintiff Desirae Broadhead is a citizen of the State of Nebraska. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

34. Plaintiff Ronald Brown is a citizen of the State of New Mexico. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

35. Plaintiff Ashlie Atkinson is a citizen of the State of New York. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

36. Plaintiff Rebekah Rhodes is a citizen of the State of North Carolina. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

37. Plaintiff Kyle Hannah is a citizen of the State of North Carolina. Upon information and belief, his personal information, including full name, Social

Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

38. Plaintiff Courtney Finch is a citizen of the State of North Carolina. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

39. Plaintiff Michael Finch is a citizen of the State of North Carolina. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

40. Plaintiff Herschel Sigall is a citizen of the State of Ohio. Upon information and belief, his personal information including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

41. Plaintiff Meredith Villines is a citizen of the State of Oregon. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

42. Plaintiff Nicholas Watson is a citizen of the Commonwealth of Pennsylvania. Upon information and belief, his personal information, including full

name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

43. Plaintiff Jessica Watson is a citizen of the Commonwealth of Pennsylvania. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

44. Plaintiff Gregory Kesden is a citizen of the Commonwealth of Pennsylvania. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

45. Plaintiff Keith Reisman is a citizen of the State of Tennessee. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

46. Plaintiff Jason Pippin is a citizen of the State of Texas. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

47. Plaintiff Robin Smith is a citizen of the State of Utah. Upon information and belief, his personal information, including full name, Social Security number,

birth date, addresses, drivers' license, and credit history was compromised in the Breach.

48. Plaintiff Anthony Dimmagio is a citizen of the State of Washington. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

49. Plaintiff Kurt Zende is a citizen of the State of West Virginia. Upon information and belief, his personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

50. Plaintiff Carol Barber is a citizen of the State of Wyoming. Upon information and belief, her personal information, including full name, Social Security number, birth date, addresses, drivers' license, and credit history was compromised in the Breach.

51. Defendant Equifax, Inc. is a publicly traded Georgia corporation headquartered in Atlanta, Georgia that regularly conducts business throughout the United States and is a national credit reporting agency.

JURISDICTION AND VENUE

52. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value

of $5,000,000 and is a class action in which there are in excess of 100 class members and the members of the Class are citizens of a state different from Defendant.

53. This Court has general and specific jurisdiction over Equifax because Equifax has sufficient minimum contacts within the State of Georgia and within the Northern District of Georgia.

54. Venue is proper in this Court pursuant to 28 U.S.C. §§1391(a) and (b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this judicial district. Venue is also proper under 18 U.S.C. §1965(a) because Defendant transacts substantial business in this District.

GENERAL ALLEGATIONS

55. Equifax is a consumer credit reporting agency in the United States. It gathers and maintains information on over 800 million consumers and more than 88 million businesses worldwide. It is one of the three largest American credit agencies, along with Experian and TransUnion.

56. On September 7, 2017, Equifax announced that a group of hackers had stolen the personal data of approximately 143 million U.S. consumers.[5] The data breach (the "Breach") lasted from the middle of May 2017 through July 2017, during

[5] https://www.wsj.com/articles/equifax-reports-data-breach-possibly-impacting-143-million-u-s-consumers-1504819765

which time the hackers managed to exploit a security flaw on Equifax's website.[6] Equifax discovered the Breach on July 29th, 2017, yet chose not to inform the public for five weeks.[7]

57. The compromised data included, at minimum, individuals' full names, Social Security numbers, birth dates, addresses, and driver license numbers. These data are critical items of personally-identifiable information ("PII"), as they are commonplace identifiers required to establish myriad financial, medical, and other transactions. Moreover, these items of PII cannot be reissued or replaced. So, once compromised, they expose individuals to profound risk, in perpetuity.

58. In addition to stealing information from the accounts of roughly 143 million consumers, the hackers also accessed the credit card numbers of about 209,000 consumers in the U.S. and other documents with personal identifying information for about 182,000 people in the U.S.[8]

59. Recognizing the gravity of the Breach, Marie White, CEO of Security Mentor, stated that:

> [The Breach could] potentially be one of the most significant data breaches in history. . . . The size of the breach, quality and quantity of personal information and

[6] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/
[7] http://www.foxbusiness.com/features/2017/09/07/equifax-143m-us-consumers-affected-by-criminal-cybersecurity-breach.html
[8] http://www.foxbusiness.com/features/2017/09/07/equifax-143m-us-consumers-affected-by-criminal-cybersecurity-breach.html

> far-reaching impact make it unprecedented. . . . Imagine if one out of every two people walking down the street dropped their credit card, along with a sticky note on the back with all their personal information needed to access that card. Now imagine that happening in every city across the country.[9]

60. Criminals now have access to the full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers of nearly 44% of the US population.[10] If children and people without credit histories are removed from this percentage, then more than half of all US residents who rely the most on bank loans and credit cards are now at a significantly higher risk of fraud and will remain so for years to come.[11] In addition, consumers' PII could be abused by hostile governments to obtain information from people with security clearances.[12]

61. Shuman Ghosemajumder, the Chief Technology Officer for Shape Security, has stated that "[t]his appears to be the single largest breach of Social Security Numbers in history."[13] He concluded that, "it is possible that as a result of this breach, the majority of adults' SSNs are now comprised."[14]

---

[9] https://www.thestreet.com/story/14298348/1/equifax-breach-of-143-million-consumers-increases-identity-theft-odds.html
[10] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/
[11] *Id.*
[12] *Id.*
[13]http://www.cetusnews.com/business/The-Morning-Download--Equifax-Breach-Puts-Social-Security-Number-at-Center-of-Digital-Identity-Crisis.HkenFAZecZ.html
[14] *Id.*

62. Equifax's five-week delay in announcing the Breach is completely unacceptable. The company has failed to even offer an explanation for the delay. Nevertheless, three Equifax executives were permitted to sell more than $1.8 million worth of stock immediately following the company's discovery of the Breach.[15]

63. Nor is this the first time Equifax has been involved in a breach that exposed sensitive consumer data. In 2013, the company confirmed that the personal details for famous people—including US Vice President Joe Biden, FBI Director Robert Mueller, Attorney General Eric Holder, and rap star Jay Z—were exposed on annualcreditreport.com, a site that allows consumers to monitor their credit reports. Lax security on the site allowed people to gain unauthorized access to other people's reports by supplying their previous addresses, mortgages, outstanding loans, and other details that are often widely known.[16]

64. Likewise, Equifax's efforts to alert consumers of the Breach has been handled extremely poorly. The website established by the company to inform consumers whether their PII has been compromised (www.equifaxsecurity2017.com) fails to provide the enterprise-grade security required for a site that asks people to provide their last name and all but three digits

[15] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

[16] https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/

of their Social Security number.[17] Moreover, the domain name isn't registered to Equifax, and the website's format resembles the kind of thing a criminal operation might use to steal people's details.[18] In fact, Cisco-owned Open DNS was blocking access to the site and warning it was a suspected phishing threat.[19]

65. Noted security researcher Brian Krebs described Equifax's response to the breach as "completely broken at best, and little more than a stalling tactic or sham at worst."[20] Of particular concern, the website the company created to inform people whether they were affected by the breach would provide results seemingly at random: "In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones."

> Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring services we were eligible for were not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.[21]

---

[17] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/
[18] *Id.*
[19] *Id.*
[20] https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/
[21] *Id.*

66. Not only is Equifax's remediation effort poorly executed, it is also a deceptive attempt to shield itself from liability. Equifax purports to offer affected consumers a year of free credit monitoring and identity theft protection, through a product called TrustedID. However, in signing up for TrustedID, consumers must agree to a terms of service that includes a binding arbitration provision and class action waiver.[22] Further, TrustedID's terms of service were updated on September 6, 2017, the day before the Breach was announced, by Equifax, to the public.

67. Once exposed, this tactic was widely decried by the public, the media, and law enforcement. The Consumer Financial Protection Bureau called Equifax's use of an arbitration provision in its remedial services "troubling" and stated that the agency is investigation not only the Breach, but also Equifax's response.[23] The New York Attorney General's Office directly confronted Equifax, maintaining that the language was unenforceable and demanding clarification.[24] Equifax then represented, on an FAQ on its website, that "[t]he arbitration clause and class action waiver included in the TrustedID Premier Terms of Use applies to the free credit monitoring and identity theft protection products, and not the cybersecurity event."

[22]http://www.slate.com/articles/technology/future_tense/2017/09/victims_of_the_equifax_hack_that_used_the_website_may_not_necessarily_be.html
[23] https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm_term=.8b564845902c
[24] https://www.cnet.com/how-to/a-guide-to-surviving-equifax-data-breach/

However, this clarification has not been incorporated into the TrustedID terms of service, which purports to constitute the entire agreement.[25]

68. Equifax's bad acts are myriad. Beyond failing to take adequate steps to protect the sensitive personal information of Plaintiffs and Class members, Equifax has also failed to disclose the nature and extent of the Breach and notify affected consumers in a timely manner, and has also attempted to trick consumers into signing away their legal rights in return for remediating services. By negligently allowing the Breach, failing to provide adequate notice, and forcing consumers into the Hobson's choice between protection and their legal rights, Equifax has prevented (and continues to prevent) Plaintiffs and Class members from protecting themselves from the security breach.

CLASS ALLEGATIONS

69. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and all others similarly situated, as representative of the following Classes:

A. The State Statutory Classes

70. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their claims that Equifax violated state consumer statutes (Count I) and state data breach notification laws (Count II) on behalf of separate statewide classes, defined as follows:

[25] https://trustedidpremier.com/static/terms

> **Statewide [Consumer Protection or Data Breach Notification] Classes:** All residents of [name of State] whose PII was compromised as a result of the data breach first disclosed by Equifax in September 2017.

71. Plaintiffs assert the state consumer law claims (Count I) under the listed consumer protection laws of Alabama, Arizona, California, Colorado, Connecticut, Florida, Hawaii, Louisiana, Maryland, Michigan, Missouri, Mississippi, Nebraska, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Utah, Washington, and West Virginia.

72. Plaintiffs assert the state data breach notification law claims (Count II) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, California, Colorado, Georgia, Hawaii, Louisiana, Maryland, Michigan, North Carolina, Oregon, Tennessee, Washington, and Wyoming.

B. The Nationwide Class

73. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their common law claims for negligence (Count III), breach of implied contract (Count IV), unjust enrichment (Count V), and declaratory judgment (Count VI) on behalf of a nationwide class, defined as follows:

> **Nationwide Class:** All residents of the United States whose PII was compromised as a result of the data breach first disclosed by Equifax in September 2017.

C. The State Common Law Classes

74. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims for negligence (Count III), breach of implied contract (Count IV), unjust enrichment (Count V), and declaratory judgment (Count VI) under the laws of the individual States and Territories of the United States, and on behalf of separate statewide classes, defined as follows:

> **Statewide [Negligence, Breach of Implied Contract, Unjust Enrichment, or Declaratory Judgment] Classes:** All residents of [name of State] whose PII was compromised as a result of the data breach first disclosed by Equifax in September 2017.

D. The California Class

75. Pursuant to Fed. R. Civ. P. 23, Plaintiffs Barbara Queenen, Maggie McKinney, and Lily Zhou (collectively, the "California Plaintiffs") assert a claim under the California Customer Records Act, California Civil Code section 1798.81.5, and the "unlawful prong" of California's Unfair Competition Law, California Business and Professions Code section 17200 (Count VII) on behalf of a California class defined as follows:

> **California Class:** All residents of California whose PII was compromised as a result of the data breach first disclosed by Equifax in September 2017.

E. The Maryland Class

76. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiff Amanda Lotts asserts a claim under the Maryland Personal Information Protection Act, Maryland Code, Commercial Law section 14-3503, and the Maryland Consumer Protection Act, Maryland Code, Commercial Law section 13-101, et seq. (Count IX), on behalf of a Maryland class defined as follows:

> **Maryland Class:** All residents of Maryland whose PII was compromised as a result of the data breach first disclosed by Equifax in September 2017.

77. Excluded from each of the above Classes is Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

78. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3):

79. **Numerosity.** The proposed Classes include, at minimum, 143 million individuals whose data was compromised in the Breach. While the precise number of Class members in each proposed class has not yet been determined, the massive size of the Equifax data breach indicates that joinder of each member would be impracticable.

80. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. whether Equifax engaged in the conduct alleged herein;

b. whether Equifax's conduct constituted Deceptive Trade Practices (as defined below) actionable under the applicable consumer protection laws;

c. whether Equifax had a legal duty to adequately protect Plaintiffs' and Class members' PII;

d. whether Equifax breached its legal duty by failing to adequately protect Plaintiffs' and Class members' PII;

e. whether Equifax had a legal duty to provide timely and accurate notice of the Equifax data breach to Plaintiffs and Class members;

f. whether Equifax breached its duty to provide timely and accurate notice of the Equifax data breach to Plaintiffs and Class members;

g. whether and when Equifax knew or should have known that Plaintiffs' and Class members' PII stored on its computer systems was vulnerable to attack;

h. whether Plaintiffs and Class members are entitled to recover actual

damages and/or statutory damages; and

i. whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

81. **Typicality.** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and Class members were injured through Equifax's uniform misconduct and their legal claims arise from the same core Equifax practices.

82. **Adequacy.** Plaintiffs are adequate representatives of the proposed classes because their interests do not conflict with the interests of the Class members they seek to represent. Plaintiffs' counsel are very experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive retail data breach cases.

83. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies

of scale, and comprehensive supervision by a single court.

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

85. Finally, all members of the purposed Classes are readily ascertainable. Equifax has access to addresses and other contact information for all members of the Classes, which can be used to identify Class members.

COUNT I
VIOLATIONS OF STATE CONSUMER LAWS
(ON BEHALF OF PLAINTIFFS AND THE SEPARATE STATEWIDE CONSUMER LAW CLASSES)

86. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

87. Plaintiffs and members of the statewide Consumer Law Classes (the "Class" for purposes of this Count) are consumers who had their PII compromised during Equifax's failure to prevent the Breach from occurring.

88. Equifax engaged in the conduct alleged in this Complaint by collecting consumers' PII for its own commercial purposes, including Plaintiffs' and members of the Class's PII.

89. 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 collecting PII from consumers throughout the United States for its own commercial purposes.

90. Equifax's conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices (collectively, "Deceptive Trade Practices"), including, among other things, Equifax's:

a. failure to maintain adequate computer systems and data security practices to safeguard customers' PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard customers' PII from theft;

c. failure to timely and accurately disclose the data breach to Plaintiffs and Class members;

91. By engaging in such Deceptive Trade Practices, Equifax has violated state consumer laws, including those that prohibit:

a. representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. representing that goods and services are of a particular standard, quality or grade, if they are of another;

c. omitting material facts regarding the goods and services sold;

d. engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;

e. unfair methods of competition;

f. unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices; and/or;

g. similar prohibitions under the state consumer laws identified below.

92. As a direct result of Equifax's violating state consumer laws, Plaintiffs and Class members suffered damages that include:

a. theft of their PII by criminals;

b. costs associated with the detection and prevention of identity theft;

c. costs associated with the fraudulent use of their financial accounts;

d. loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

e. costs and lost time associated with handling the administrative consequences of the Equifax data breach, including identifying, disputing, and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit

monitoring and identity theft protection;

f. impairment to their credit scores and ability to borrow and/or obtain credit; and

g. the continued risk to their personal information, which remains on Equifax's insufficiently secured computer systems.

93. Equifax's Deceptive Trade Practices violate the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19- 5(2), (3), (5), (7), and (27), *et seq.*;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq*.;

d. The Colorado Consumer Protection Act, Col. Rev. Stat. Ann. §§ 6-1-105(1)(b), (c), (e) and (g), *et seq*.;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

f. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

g. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq*., and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq*.;

h. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq*.;

i. The Maryland Consumer Protection Act, Md. Code Commercial Law, §§ 13-301(1) and (2)(i)-(ii), and (iv), (5)(i), and (9)(i), *et seq*.;

j. The Michigan Consumer Protection Act, M.C.P.L.A. §§ 445.903(1)(c)(e), (s) and (cc), *et seq*.;

k. The Mississippi Consumer Protect Act, Miss. Code Ann. §§ 75-24-5(1), (2)(b), (c), (e), and (g), *et seq*.;

l. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq*.;

m. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq*.;

n. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57- 12-2(D)(5)(7) and (14) and 57-12-3, *et seq*.;

o. The New York Business Law, N.Y. Gen. Bus. Law § 349(a);

p. The North Carolina Unfair Trade Practices Act, N.C.G.S.A. § 75- 1.1(a), *et seq.*;

q. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. §§ 1345.02(A) and (B)(1) and (2), *et seq.*;

r. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. §§ 646.608(1)(e)(g) and (u), *et seq.*;

s. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;

t. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a), (b)(2), (3), (5), and (7), *et seq.*;

u. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13- 11-4(1), (2)(a), (b), and (i) *et seq.*;

v. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.*; and

w. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq.*

94. As a result of Equifax's violations, Plaintiffs and members of the Class are entitled to injunctive relief, including, but not limited to: (1) ordering

that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax segment customer data by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax's systems; (5) ordering that Equifax purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Equifax conduct regular database scanning and securing checks; (7) ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Equifax to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

95. Because of Equifax's Deceptive Trade Practices, Plaintiffs and the

Class members are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Equifax because of its Deceptive Trade Practices, attorneys' fees and costs, declaratory relief, and a permanent injunction enjoining Equifax from its Deceptive Trade Practices.

96. Plaintiffs bring this claim on behalf of themselves and the Class members for the relief requested and to benefit the public interest. This claim supports the public interests in assuring that consumers are provided truthful, non-deceptive information about potential purchases and protecting members of the public from Equifax's Deceptive Trade Practices. Equifax's wrongful conduct, including its Deceptive Trade Practices has affected the public at large because a substantial percentage of the U.S. population has been affected by Equifax's conduct.

97. Plaintiffs have provided notice of this action and a copy of this Complaint to the appropriate Attorneys General pursuant to Conn. Gen. Stat. § 42-110g(c); Ore. Rev. Stat. Ann. § 646.638(s); and Wash. Rev. Code § 19.86.095.

COUNT II
VIOLATIONS OF STATE DATA BREACH NOTIFICATION STATUTES (ON BEHALF OF PLAINTIFFS AND THE SEPARATE STATEWIDE DATA BREACH STATUTE CLASSES)

98. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

99. Legislatures in the states and jurisdictions listed below have enacted

data breach statutes. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

100. The Equifax data breach constituted a security breach that triggered the notice provisions of the data breach statutes and the PII taken includes categories of personal information protected by the data breach statutes.

101. Equifax unreasonably delayed in informing Plaintiffs and members of the statewide Data Breach Statute Classes ("Class," as used in this Count), about the data breach after Equifax knew or should have known that the data breach had occurred.

102. Plaintiffs and Class members were damaged by Equifax's failure to comply with the data breach statutes.

103. Had Equifax provided timely and accurate notice, Plaintiffs and Class members could have avoided or mitigated the harm caused by the data breach. For example, they could have taken security precautions in time to prevent or minimize identity theft.

104. Equifax's failure to provide timely and accurate notice of the Equifax

data breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Cal. Civ. Code § 1798.80, *et seq.*;

c. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

d. Ga. Code Ann. § 10-1-912(a), *et seq.*;

e. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

f. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

g. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

h. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

i. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

j. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

k. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

l. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*; and

m. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

105. Plaintiffs and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to damages, equitable relief, including injunctive relief, treble damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

COUNT III
NEGLIGECE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE NEGLIGENCE CLASSES)

106. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

107. Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, or, alternatively, members of the Separate Statewide Negligence Classes (collectively, the "Class" as used in this Count). Equifax's duties included the following:

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

b. to protect their PII using reasonable and adequate security procedures and systems that are compliant and consistent with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class members of the Equifax data breach.

108. Equifax owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Equifax

solicited, gathered, and stored Plaintiffs' and Class members' PII for its commercial purposes.

109. Equifax knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Equifax received warnings from within and outside the company that hackers routinely attempted to access Personal Information without authorization. Equifax also knew about numerous, well-publicized data breaches by other companies.

110. Equifax knew, or should have known, that its computer systems did not adequately safeguard Plaintiffs' and Class members' PII.

111. Because Equifax knew that a breach of its systems would damage millions of consumers, including Plaintiffs and Class members, it had a duty to adequately protect their PII.

112. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its point-of-sale systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) employ adequate network segmentation, (4) implement adequate system and event monitoring, and (5) implement the systems, policies, and procedures necessary to prevent this type of data breach.

113. Equifax also had independent duties under state laws that required

Equifax to reasonably safeguard Plaintiffs' and Class members' PII and promptly notify them about the data breach.

114. Equifax breached the duties it owed to Plaintiffs and Class members in numerous ways, including:

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

b. by failing to implement adequate security systems, protocols and practices sufficient to protect their PII both before and after learning of the data breach;

c. by failing to comply with the minimum industry data security standards, during the period of the data breach; and

d. by failing to timely and accurately disclose that their PII had been improperly acquired or accessed.

115. But for Equifax's wrongful and negligent breach of the duties it owed Plaintiffs and Class members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

116. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Equifax's negligent conduct. Accordingly, Plaintiffs and the Class have suffered injury and are entitled to

damages in an amount to be proven at trial.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE BREACH OF IMPLIED CONTRACT CLASSES)

117. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

118. When Plaintiffs and the members of the Nationwide class or, alternatively, the members of the Separate Statewide Breach of Implied Contract Classes (collectively, the "Class" as used in this Count), provided their PII to Equifax to obtain credit reports, they entered into implied contracts by which Equifax agreed to protect their PII and timely notify them in the event of a data breach.

119. Equifax invited consumers, including Plaintiffs and Class members, to provide their PII to Equifax to obtain credit reports. The PII was valuable to Equifax, because Equifax uses it for ancillary marketing and business purposes.

120. An implicit part of the offer was that Equifax would safeguard the PII using reasonable or industry-standard means and would timely notify Plaintiffs' and the Class in the event of a data breach.

121. Equifax also affirmatively represented that it collected consumers' PII when they provided that information in exchange for credit reports, used that information for a variety of business purposes, and protected the PII using "industry

standard means."

122. Based on the implicit understanding and also on Equifax's representations, Plaintiffs and the Class accepted the offers and provided Equifax with their PII by providing them with that information in exchange for credit reports during the period of the Equifax data breach.

123. Plaintiffs and Class members would not have provided their PII to Equifax had they known that the company would not safeguard their PII as promised or provide timely notice of a data breach.

124. Plaintiffs and Class members fully performed their obligations under the implied contracts with Equifax.

125. Equifax breached the implied contracts by failing to safeguard Plaintiffs' and Class members' PII and failing to provide them with timely and accurate notice when their PII was compromised in the data breach.

126. The losses and damages Plaintiffs and Class members sustained (as described above) were the direct and proximate result of Equifax's breaches of its implied contracts with them.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE UNJUST ENRICHMENT CLASSES)

127. Plaintiffs reallege, as if fully set forth, the allegations set forth in all

paragraphs above.

128. Plaintiffs and members of the Nationwide class or, alternatively, the members of the Separate Statewide Unjust Enrichment Classes (collectively, the "Class" as used in this Count), conferred a benefit on Equifax. Specifically, they provided Equifax with (or otherwise allowed Equifax the use of) their PII in exchange for credit reports. In exchange, Plaintiffs and Class members should have been protected by having Equifax process and store their PII using adequate data security.

129. Equifax knew that Plaintiffs and the Class conferred a benefit on Equifax. Equifax profited from using their PII for its own business purposes.

130. Equifax failed to secure the Plaintiffs' and Class members' PII, and, therefore, did not safeguard the benefit the Plaintiffs and Class members provided.

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

132. Had Plaintiffs and Class members known that Equifax would not secure their PII using adequate security, they would not have furnished their PII (or allowed their PII to be furnished) to Equifax.

133. Plaintiffs and the Class have no adequate remedy at law.

134. Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits that Plaintiffs and Class members of the Class conferred on it.

135. Equifax should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class members proceeds that it unjustly received from them or as a result of receiving their data. In the alternative, Equifax should be compelled to refund any amounts that Plaintiffs and the Class may have paid.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE SEPARATE STATEWIDE NEGLIGENCE AND BREACH OF IMPLIED CONTRACT CLASSES)

136. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

137. As previously alleged, Plaintiffs and members of the Breach of Implied Contract classes entered into an implied contract that required Equifax to provide adequate security for the PII it collected from them. As previously alleged, Equifax owes duties of care to Plaintiffs and the members of the Nationwide class or, alternatively, the separate statewide Negligence classes, that require it to adequately secure PII.

138. Equifax still possesses PII regarding the Plaintiffs' and the Class members.

139. After the Equifax data breach, Equifax announced changes that it claimed would improve data security. These changes, however, did not fix many

systemic vulnerabilities in Equifax's computer systems.

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

141. Actual harm has arisen in the wake of Equifax's data breach regarding its contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Breach of Implied Contract and Negligence Classes. Equifax maintains that its security measures now are adequate even though the changes it announced were insufficient to meet Equifax's contractual obligations and legal duties.

142. Plaintiffs, therefore, seek a declaration (a) that Equifax's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (b) that to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to: (1) ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Equifax

engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax segment customer data by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax's systems; (5) ordering that Equifax purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Equifax conduct regular database scanning and securing checks; (7) ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Equifax to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

COUNT VII
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, CALIFORNIA CIVIL CODE § 1798.81.5 AND THE CALIFORNIA UNFAIR COMPETITION LAW'S UNLAWFUL PRONG (ON BEHALF OF THE CALIFORNIA PLAINTIFFS AND THE CALIFORNIA CLASS)

143. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

144. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act, California Civil Code §1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

145. As described above, Equifax failed to implement and maintain reasonable security procedures and practices to protect the California Plaintiffs' and California Class members' personal information, and thereby violated California Civil Code section 1798.81.5.

146. By violating section 1798.81.5 of the California Customer Records Act, Equifax is liable to the California Plaintiffs and California Class members for damages under California Civil Code section 1798.84(b).

147. Because Equifax "violates, proposes to violate, or has violated," the California Customer Records Act, California Plaintiffs are entitled to injunctive relief under California Civil Code section 1798.84(e).

148. In addition, Equifax's violations of the Customer Records Act constitute unlawful acts or practices under California's Unfair Competition Law, California Business and Professions Code sections 17200, et seq., which provides

for restitution damages, and grants the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

149. Accordingly, the California Plaintiffs request that the court enter an injunction that requires Equifax to implement reasonable security procedures and practices, including, but not limited to: (1) ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax segment customer data by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax's systems; (5) ordering that Equifax purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Equifax conduct regular database scanning and securing checks; (7) ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Equifax to

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

150. California Plaintiffs and members of the California Class seek all remedies available under the California Customer Records Act and the California Unfair Competition Law, including but not limited to, restitution, damages, equitable relief, including injunctive relief, reasonable attorneys' fees and costs, and all other relief allowed under the applicable laws.

COUNT VIII
VIOLATION OF THE MARYLAND PERSONAL INFORMATION PROTECTION ACT AND CONSUMER PROTECTION ACT, MARYLAND CODE COMMERCIAL LAW §§ 13-101 ET SEQ., 14-3501 ET SEQ. (ON BEHALF OF PLAINTIFF AMANDA LOTS AND THE MARYLAND CLASS)

151. Plaintiffs reallege, as if fully set forth, the allegations set forth in all paragraphs above.

152. "[T]o protect personal information from unauthorized access, use, modification, or disclosure," the Maryland Legislature enacted the Personal Information Protection Act, Maryland Code, Commercial Law § 14-3503(a), which requires that any business that "owns or licenses personal information about a [Maryland resident] shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."

153. As described above, Equifax failed to implement and maintain reasonable security procedures and practices to protect Plaintiff Lots' and the Maryland Class members' personal information, and thereby violated Maryland Code, Commercial Law section 14-3503(a).

154. Under Maryland Code, Commercial Law section 14-3508, Equifax's violations of the Maryland Personal Information Protection Act also constitute unfair or deceptive trade practices prohibited by the Maryland Consumer Protection Act, and subject to the Consumer Protection Act's enforcement provisions.

155. Accordingly, Equifax is liable to Plaintiff Lots and the Maryland Class members for damages and attorneys' fees under Maryland Code, Commercial Law section 13-408.

156. Plaintiff Lots and the Maryland Class members seek all remedies available under Maryland law, including but not limited to, damages and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes, respectfully request that the Court enter judgment in their favor that:

A. certifies the Classes requested, appoints the Plaintiffs as class representatives of the applicable classes and the Court-appointed Liaison Counsel and Co-Lead Counsel Representing Consumer Plaintiffs as

Class counsel;

B. awards the Plaintiffs and Class members appropriate monetary relief, including actual and statutory damages, restitution, and disgorgement,

C. on behalf of Plaintiffs and the Statewide Consumer Classes, enters an injunction against Equifax's Deceptive Trade Practices and requires Equifax to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Plaintiffs' PII, which remains in the possession of Equifax;

D. on behalf of Plaintiffs and the Statewide Data Breach Statute Classes, awards appropriate equitable relief, including an injunction requiring Equifax to promptly notify all affected customers of future data breaches;

E. orders Equifax to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

F. awards Plaintiffs and the Classes pre-judgment and post- judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

G. awards such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Respectfully submitted this 12th day of September, 2017.

COMPLEX LAW GROUP, LLC

By: /s/ David M. Cohen
David M. Cohen
Ga. Bar No. 173503
40 Powder Springs Street
Marietta, GA 30064
Telephone: (770) 200-3100
Facsimile: (770) 200-3101
dcohen@complexlaw.com

CARNEY BATES & PULLIAM, PLLC

Allen Carney (to be admitted *pro hac vice*)
519 W. 7th Street
Little Rock, AR 72201
Telephone: (501) 312-8500
Facsimile: (501) 312-8505
acarney@cbplaw.com

Attorneys for Plaintiffs and Proposed Classes

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Andrew McDowell et al.,

(b) County of Residence of First Listed Plaintiff Madison, AL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Complex Law Group, LLC
40 Powder Springs Street
Marietta, Georgia 30064 770-200-3100

DEFENDANTS

Equifax, Inc.

County of Residence of First Listed Defendant Fulton County, Georgia
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☒ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act 28 U.S.C. 1332 (d)(2)

Brief description of cause:
Consumer Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Hon. William S. Duffey, Jr. DOCKET NUMBER 1:17-cv-03422

DATE
09/12/2017

SIGNATURE OF ATTORNEY OF RECORD
/s/ David M. Cohen

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.