UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOSÉ ATILES and LAUREN SOLIN, individually and on behalf of all others similarly situated, Plaintiffs vs. EQUIFAX, INC. and EQUIFAX INFORMATION SERVICES LLC, Defendants.	No. 17 CV 7493 Jury Demand ECF Case

CLASS ACTION COMPLAINT

MULLEN P.C.
Wesley M. Mullen (WM1212)
200 Park Avenue | Suite 1700
New York, NY 10166
(646) 632-3718
wmullen@mullenpc.com

TABLE OF CONTENTS

> *People across the country and around the world, including our friends and family members, put their trust in our company. We didn't live up to expectations. We were hacked. That's the simple fact.*
>
> *But we compounded the problem … .*[1]
>
> Paulino do Rego Barros, Jr.
>
> Interim CEO, Equifax Inc.
> Wall Street Journal, Sept. 27, 2017

Plaintiffs JOSÉ ATILES and LAUREN SOLIN, by their attorneys, for their Class Action Complaint against Defendants EQUIFAX, INC. and EQUIFAX INFORMATION SERVICES LLC allege as follows:

NATURE OF THE CASE

1. This is a class action brought on behalf of New York, New Jersey and other U.S. citizens whose personally identifiable information ("PII") was stolen by criminals as a direct result of the actions and culpable failures to act of Defendants Equifax, Inc. and its subsidiary Equifax Information Services LLC (collectively, "Equifax" or the "Company").

2. On September 7, 2017, Equifax announced that hackers had exploited a known software vulnerability (the "Data Breach") and obtained the PII of approximately 143 million Americans,

[1] Paulino do Rego Barros Jr., On Behalf of Equifax, I'm Sorry, Wall Street Journal, Sept. 27, 2017, available at http://on.wsj.com/2x3w1Rj.

including over 8 million New Yorkers and over 4 million New Jerseyans.

3. According to Equifax's own public statements about the Data Breach, hackers obtained millions of U.S. consumers' names, birth dates, social security numbers ("SSNs"), addresses, and in some cases, drivers' license numbers. The hackers also obtained credit card numbers for approximately 209,000 U.S. consumers and credit dispute documents for another 182,000.

4. Equifax first discovered the intrusion on July 29, 2017. The Company reported that the hackers responsible for the Data Breach took advantage of a known vulnerability in an open-source software package called Apache Struts (CVE-2017-5638).

5. Apache – a third-party software developer – knew of the vulnerability as early as March 8, 2017, and advised customers and users (including Equifax) to update the software in order to prevent unauthorized access. Equifax, however, neglected to implement the patch until more than four months later – after its failure to do so had already resulted in the Data Breach. "In other words, the credit-reporting giant had more than two months to take precautions that would

have defended the personal data of 143 million people from being exposed. It didn't."[2]

6. As a result of Equifax's failure to patch a known vulnerability in its data security measures, hackers gained unauthorized access to Equifax's computer systems from at least May 13, 2017 through July 30, 2017.

7. Even after the Data Breach, Equifax has not provided adequate measures for affected consumers to mitigate damages caused by the Data Breach and to protect themselves against further harm. As Equifax's Interim CEO stated in the Wall Street Journal: "We were hacked. That's the simple fact. But we compounded the problem with insufficient support for consumers."

8. Equifax waited nearly six weeks after it discovered the data breach to publicly disclose the incident. During that time, millions of consumers remained unaware that their PII had been stolen and that it was vulnerable to misuse by bad actors.

9. When it at last disclosed the Data Breach, Equifax set up a website at www.equifaxsecurity2017.com for consumers to use to identify whether their PII had been stolen. But the Company badly botched the effort. To use the website and to check

[2] Lily Hay Newman, Equifax Officially Has No Excuse, Wired (Sept. 14, 2017), available at http://bit.ly/2x1axDI.

whether their PII had been compromised, consumers were required consumers to enter their last name and the last six digits of their SSN. Due to the sensitive nature of the information Equifax requests, consumers are led to believe that they are giving their PII to a trustworthy party. Equifax breached that trust by carelessly tweeting a link to a phishing website (www.securityequifax2017.com) instead of Equifax's own.

10. Equifax had statutory and common-law obligations to protect the PII of consumers. Yet it failed at every step to prevent, detect or limit the scope of the Data Breach. Equifax was well aware of the threat of cyber attacks and was or should have been on full notice of its cybersecurity vulnerabilities, having previously experienced a breach in its TALX division in March 2017. Nevertheless, Equifax (a) failed to implement software updates for a known security vulnerability; (b) failed to detect unauthorized intrusions into its computer systems; (c) failed promptly and adequately to notify consumers of the Data Breach; and (d) failed to provide consumers with adequate measures to mitigate the harms caused by, or protect against future harms caused by, the Data Breach.

11. Equifax concealed the weaknesses in its security systems, was negligent in safeguarding consumer data, and violated New York and New Jersey law, including New York General

Business Law § 349; the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2; and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. § 56:8-163(b).

12. As a direct result of the data breach, Plaintiffs and the Class suffered damages, including (a) costs associated with the detection and prevention of identity theft and unauthorized use of their personal and financial information; and (b) the imminent and impending costs from future fraud and identity theft.

PARTIES

13. Plaintiff JOSÉ ATILES ("Atiles") is a citizen of New York State and New York City. He resides in the Bronx. Mr. Atiles provided sensitive information to Defendants, including his SSN, current and former addresses, date of birth, and other identifying information, in order to receive one or more credit reports and in connection with the purchase of access to view his credit score. Upon information and belief, Mr. Atiles's SSN and other PII were exposed by Equifax in the Data Breach. Upon learning of the breach, Mr. Atiles suffered considerable anxiety and confusion concerning the vulnerability of his PII. He consulted attorneys and purchased credit monitoring services to protect himself from further harm as a result of Defendants' Data Breach.

14. Plaintiff LAUREN SOLIN is a citizen of New Jersey resident in Fairlawn, New Jersey. Ms. Solin provided sensitive information to Defendants, including her SSN, current and former addresses, date of birth, and other identifying information, in order to receive one or more credit reports and in connection with the purchase of access to view her credit score. Upon information and belief, Ms. Solin's SSN and other PII were exposed by Equifax in the Data Breach. Upon learning of the breach, Ms. Solin suffered considerable anxiety and confusion concerning the vulnerability of her PII. She consulted attorneys and purchased credit monitoring services to protect herself from further harm as a result of Defendants' Data Breach.

15. Defendant Equifax, Inc. is a Georgia corporation with its principal place of business at 1550 Peachtree Street NW, Atlanta, Georgia 30309.

16. Defendant Equifax Information Services LLC is a subsidiary of Equifax, Inc. that collects consumer information and reports that information to financial institutions. Equifax Information Services LLC is incorporated in Georgia and maintains its principal place of business at 1550 Peachtree Street NW, Atlanta, Georgia 30309.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (i) this is a class action in which the matter in controversy exceeds $5 million, exclusive of interest and costs; (ii) there are more than one hundred class members; and (iii) Plaintiffs and the Class are citizens of different states than at least one defendant, satisfying the statutory minimal diversity requirement.

18. Venue is proper in this District under 28 U.S.C. § 1391 because Equifax is subject to personal jurisdiction in the Southern District of New York and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Plaintiffs' provision of information to Defendants, purchase and/or use of Defendants' services, and purchase of credit monitoring services as a result of the Data Breach. Equifax provides consumer reporting and credit monitoring services to consumers in the District; maintains offices and employs workers in the District; and advertises in the District.

FACTUAL ALLEGATIONS

Equifax Stores Millions of Consumers' Most Sensitive Data

19. Equifax is one of three primary credit reporting agencies ("CRAs") in the United States. It collects, organizes and analyzes data on more than 820 million consumers worldwide. Together with the two other major CRAs, Equifax has gathered credit histories and PII for nearly every adult in the United States.

20. As part of its credit reporting business, Equifax gains access to a wide range of personal information that Equifax and its customers use to make creditworthiness judgments about consumers. Those judgments directly affect decisions on employment, loans and housing. On that basis, Equifax's website advertises the Company as part of the "essential decision-making fabric" for the world of consumer finance.

21. Equifax also solicits lenders, creditors and other businesses to provide Equifax with consumer data on a regular basis. In doing so, Equifax operates as a data broker: it seeks to maintain the integrity of its consumer files. Since Equifax's brand value and market capitalization depend heavily on the consumer data the Company has amassed, Equifax has steep economic incentives to maintain the greatest amount of

information possible on the broadest possible class of consumers.

22. By collecting and storing for profit an extensive, detailed and personal database of consumer data, Equifax is obligated to use all reasonable means to protect this data from falling into the hands of hackers and criminals. Equifax's failure to implement reasonable security measures permitted the largest consumer data breach in 2017, and possibly in history.

Equifax Knew it Faced High Risk of Attacks on its Data

23. Over recent years, data custodians in many industries have experienced breaches involving the theft of consumers' and customers PII. These breaches threaten the security and economic well-being of the affected persons. Industry actors and regulators alike have noted that data breaches are not limited to particular sectors of the economy: they impact data stewards and processors across industries including healthcare, financial services, retail and government.

24. These important trends should have – and did in fact – put Equifax on high alert. In New York, for example, the main causes of data breaches are hacking, which accounted for 40% of data security breaches reported to the Office of the New York Attorney General in 2016, and employee negligence, which accounted for 37% of reported breaches.

25. In response, regulators have called for implementation of cybersecurity measures across all industries. The Federal Trade Commission has observed that security is not a one-and-done proposition; reasonable security measures require ongoing vigilance, and carry an obligation to update and patch third-party software.[3]

26. Equifax has also conceded that security is a key tenet of its role as a trusted data steward. In recent presentations to investors, it highlighted the need for "continued investments to address critical data security throughout the [C]ompany."[4]

27. Despite its representations, Equifax itself has a history of failing adequately to protect consumer data. Prior to the Data Breach, Equifax was vulnerable to data breaches including a hack in March 2017 during which Equifax's subsidiary TALX released employee data including W-2 records to unauthorized users.[5]

28. In response to that incident – which resulted from hackers resetting employees' four-digit PIN numbers – security researchers condemned Equifax's failure to implement even the

[3] See Start With Security: A Guide for Business, FTC (Jun. 2014), available at http://bit.ly/1dvaCRX.

[4] Equifax, Inc. Investor Relations Presentation (June 2017), available at http://bit.ly/2yNtY11.

[5] See TALX Disclosure re: Data Security Incident (May 15, 2017), available at http://bit.ly/2kfx626.

most basic security measures, such as two-factor authentication ("2FA"), to protect the sensitive information in its database. "It's pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN."[6]

29. In light of the industry-wide history of cyber attacks, including numerous high-profile consumer data breaches and regulator warnings, Equifax plainly should have known that its security practices were inadequate due to the scope and value of the consumer data in its possession. Defendants' own history of breaches and statements by the Company following those failures demonstrate that Equifax in fact knew of the risks that led to the Data Breach. It simply failed to act on them.

Equifax's Inadequate Security Caused a Massive Data Breach

30. The Equifax Data Breach is an unprecedented event. It represents one of the largest releases of personally sensitive information in recent years, and is the third major cybersecurity threat for Equifax since 2015.[7] The scale of the Data Breach has security experts operating under the assumption

[6] Brian Krebs, Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division, Krebs on Security (May 18, 2017), available at http://bit.ly/2pZ3UuJ.

[7] Tara Siegel Bernard, Equifax Says Cyberattack May Have Affected 143 Million in the U.S., The New York Times (Sept. 7, 2017).

that "everyone's Social Security number has been compromised and their identity data has been stolen."[8]

31. On September 7, 2017, Equifax first disclosed that its computer systems had been breached.

32. Equifax learned of the intrusion into its systems in late July.

33. According to Equifax disclosures, the breach occurred between May 13, 2016 and July 30, 2017, resulting in theft of PII of approximately 143 million Americans.

34. The lapse of time between July 30 and September 7 represents over a month's delay between when Equifax discovered the Data Breach and when it disclosed it. It represents an approximately two and a half month delay between when the Data Breach began and when Equifax brought it to public light.

35. As a result of the Data Breach, the hackers obtained names, birthdays, SSNs, addresses, and in some cases, driver license numbers. The attackers also gained unauthorized access to credit card numbers for more than 200,000 consumers.

[8] Lily Hay Newman, The Equifax Breach Exposes America's Identity Crisis, Wired (Sept. 8, 2017).

36. The massive Data Breach could have been entirely prevented if Equifax had taken reasonable and necessary steps to protect the sensitive consumer data in its computer systems.

CLASS ACTION ALLEGATIONS

37. Plaintiffs Atiles and Solin bring this class action on behalf of themselves and a Nationwide Class of all others similarly situated, defined as follows:

> **Nationwide Class:** All persons who are residents of the United States and its territories whose personally identifiable information and/or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

38. Plaintiff Atiles brings this class action on behalf of himself and a similarly situated New York Class, defined as follows:

> **New York Class:** All persons who are residents of New York whose personally identifiable information and/or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

39. Plaintiff Solin brings this class action on behalf of herself and a similarly situated New Jersey Class, defined as follows:

> **New Jersey Class:** All persons who are residents of New Jersey whose personally identifiable information and/or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

40. Excluded from each Class are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries and assigns. Also excluded from the Class are any judges or judicial officers presiding over this matter and the members of their immediate families.

41. This action is brought and may properly be maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

Numerosity and Ascertainability

42. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(1). Equifax admits there are at least 143 million individuals affected by the Data Breach nationwide, and numerous victims in New Jersey and New York. Many of those individuals, like Plaintiffs, depended on Equifax for credit alerts and/or

identify protection services. Individual joinder of all Class members is impracticable.

43. Each of the Classes is ascertainable because its members can readily be identified using sales records, production records, or other information kept by Defendants or third parties in the usual course of business and within their control. (Indeed, Defendants are obligated by data breach notification laws of many states to compile such information in order to notify affected and potentially affected consumers.) Plaintiffs anticipate providing appropriate notice to each certified Class in compliance with Fed. R. Civ. P. 23(c)(2)(A) and/or (B), to be approved by the Court after class certification, or pursuant to court order under Fed. R. Civ. P. 23(d).

Commonality and Predominance of Class Issues

44. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because questions of law and fact that have common answers that are the same for each of the respective Classes predominate over questions affecting only individual Class members. These common issues include but are not limited to the following:

(a) Whether Equifax owed a duty to Class members under federal or state law to protect PII; to provide timely notice of unauthorized access to data in its

possession or control; to provide timely and accurate information as to the extent of the breach; and to provide meaningful and fair redress;

(b) Whether Equifax owed a contractual duty to Class members to protect PII; to provide timely notice of unauthorized access to data in its possession or control; to provide timely and accurate information as to the extent of the breach; and to provide meaningful and fair redress;

(c) Whether Equifax breached its duty;

(d) Whether Equifax was negligent in failing to employ, design or maintain adequate security measures, systems and protocols to insure the protection of the Class' PII;

(e) Whether Defendants' negligence contributed to the Data Breach;

(f) Whether Defendants knew or should have known about the 'vulnerabilities' identified in Equifax's statements about the Data Breach that allowed criminals to gain unauthorized access to the Class' PII;

(g) Whether Defendants knew or should have known that safeguards they employed to protect the Class' PII were insufficient;

(h) Whether Defendants' actions and failures to act violated applicable state consumer protection laws;

(i) Whether Defendants' actions and failures to act violated applicable state data breach notification laws;

(j) Whether Defendants' actions violated applicable federal consumer and identity protection laws;

(k) Whether Defendants acted appropriately in securing Plaintiffs' and Class members' personal information;

(l) Whether Defendants' actions and failures to act were the proximate cause of Class members' injuries;

(m) Whether Defendants acted with reckless disregard for the safety and security of Class members' PII;

(n) Whether Class members' injuries were exacerbated by Defendants' failure timely and accurately to provide notice of the breach;

(o) Whether Defendants' public representations that they would protect Class members' PII were false;

(p) Whether Defendants' unlawful and risky practices harmed Plaintiffs and the Classes;

(q) Whether Defendants breached their contractual duties of good faith and fair dealing by failing timely to notify Class members of the breach;

(r) Whether Defendants placed unreasonable and unlawful terms and conditions on consumers' efforts to obtain information from Equifax about the extent to which Equifax itself had compromised their PII;

(s) Whether Defendants have been unjustly enriched by their conduct;

(t) Whether Plaintiffs and other Class members overpaid for Equifax services in light of Defendants' improper handling of PII;

(u) Whether Plaintiffs and other Class members are entitled to damages and other monetary relief, and if so, in what amount;

(v) Whether Plaintiffs and other Class members are entitled to declaratory relief; and

(w) Whether Plaintiffs and the Classes are entitled to equitable relief, including a preliminary or permanent injunction.

Typicality

45. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because Plaintiffs' claims are typical of the claims of Class members, and arise from the same course of conduct by Defendants. The relief Plaintiffs seek is typical of the relief sought for the absent Class members.

Adequacy of Representation

46. Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel with substantial consumer privacy law expertise and experience litigating class actions.

47. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes. Neither Plaintiffs nor their counsel have interests adverse to those of the Classes.

Superiority

48. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendants have acted and refused to act on grounds generally applicable to each Class, such that final injunctive and/or corresponding declaratory relief with respect to each Class as a whole is appropriate.

49. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The common questions of law and fact regarding Defendants' conduct and responsibility predominate over any questions affecting only individual Class members.

50. Because the damages suffered by any individual Class member may prove relatively small, the expense and burden of individual litigation would make it difficult or impossible for individual Class members to redress wrongs done to each of them individually. Most or all Class members would have no rational economic interest in individually controlling the prosecution of a specific action, and the burden imposed on the judicial system by individual litigation by even a small subset of the Class would be enormous. Class adjudication is therefore the superior alternative under Fed. R. Civ. P. 23(b)(3)(A).

51. Conduct of this action as a class action presents fewer management difficulties, better conserves judicial resources and the resources of the parties, and more effectively protects the rights of each Class member than would piecemeal litigation. Compared to the expense, burden, inconsistency, economic infeasibility, and inefficiency of individual litigation, the challenges of managing this action as a class action are outweighed by the benefits to the legitimate interest of the parties, the Court, and the public of class treatment in this Court. Class adjudication is therefore the superior alternative under Fed. R. Civ. P. 23(b)(3)(D).

52. Plaintiffs are not aware of any obstacle likely to be encountered in the management of this action that would preclude

its maintenance as a class action. Rule 23 provides the Court with authority and flexibility to maximize the efficiency and benefit of the class mechanism and to reduce management challenges. The Court may, on motion of Plaintiffs or sua sponte, certify a Nationwide Class, a New York Class and a New Jersey Class for claims sharing common legal questions; use the provisions of Rule 23(c)(4) to certify any particular claim, issue or common question of fact or law for classwide adjudication; certify and adjudicate bellwether Class claims; and utilize Rule 23(c)(5) to divide any Class into subclasses.

COUNT I

FAIR CREDIT REPORTING ACT ("FCRA")

53. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

54. Plaintiffs assert this cause of action against Defendants on behalf of members of the Nationwide Class. In the event a Nationwide Class cannot be maintained on this cause of action, the claim is asserted by Atiles on behalf of the New York Class and by Solin on behalf of the New Jersey Class.

55. PII disclosed by Defendants in the Data Breach was a "consumer report" within the meaning of the Fair Credit Reporting Act ("FCRA"). 15 U.S.C. § 1681 et seq. Such PII was

a communication of information bearing on the creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living of Plaintiffs and members of the Class that was expected to be used or collected to serve as a factor in establishing Plaintiffs' and Class members' eligibility for credit. Id. § 1681a(d)(1) (defining "consumer report").

56. Defendants are consumer reporting agencies within the meaning of the FCRA because they regularly engage, for monetary fees, in assembling and evaluating consumer credit information and other consumer information for the purpose of furnishing consumer reports to third parties such as banks, cell phone carriers and other lenders. 15 U.S.C. § 1681e(a).

57. Defendants knew or had reason to know that Plaintiffs and the Class would reasonably rely on their misrepresentations and omissions.

58. Under the FCRA, Defendants were required to maintain reasonable procedures designed to limit the furnishing of a consumer report to the six circumstances described as permissible statutory "purposes" set forth at 15 U.S.C. § 1681b.

59. Defendants violated the FCRA by furnishing PII consumer reports to unauthorized individuals or entities during the Data Breach. Furnishing consumer reports in such

circumstances is not one of the permitted purposes set forth at 15 U.S.C. § 1681b.

60. Defendants violated the FCRA by failing to maintain reasonable technological or other procedures to prevent unlawful furnishing of consumer reports.

61. Given Defendants' knowledge, experience and claimed expertise in consumer data security; given prior failures of Defendants' systems; given that the Data Breach affected a vast swath of information pertaining to essentially all U.S. adults; given that the Data Breach continued for months without detection; and given that the Data Breach, once known to Defendants, was kept secret for more than a month prior to disclosure, Defendants acted willfully or recklessly in connection with the Data Breach at issue in this action.

62. Defendants' willful and/or reckless violations of the FCRA allowed third parties to access, obtain and misuse Plaintiffs' and Class members' PII without authorization and for purposes not permitted under the FCRA.

63. Defendants' violations of their duties under the FCRA constitute de facto injuries to Plaintiffs and Class members.

64. Defendants' violations of the FCRA have directly and proximately injured Plaintiffs and Class members, including by

foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised; to take steps to minimize the extent to which the Data Breach puts their credit, reputation and finances at risk; and to take steps – now and in the future – to redress fraud, identity theft and similar foreseeable consequences of PII in the possession of hackers and criminals.

65. Pursuant to 15 U.S.C. § 1681n(a), Plaintiffs and each Class member are entitled to recover actual damages or statutory damages of not less than $100 nor more than $1,000, plus costs and attorney's fees.

COUNT II

NEGLIGENCE

66. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

67. Plaintiffs assert this cause of action against Defendants on behalf of members of the Nationwide Class. In the event a Nationwide Class cannot be maintained on this cause of action, the claim is asserted by Atiles on behalf of the New York Class and by Solin on behalf of the New Jersey Class.

68. Equifax owed Plaintiffs and the members of the Classes a duty of care commensurate to foreseeable risks of disclosure of sensitive PII, loss of sensitive PII, and injuries that would be directly and proximately caused thereby. Equifax created this duty by its voluntary and for-profit actions in collecting and storing PII for its own benefit. Equifax further created this duty by its assurances, including to Plaintiffs and the Classes, that it would safeguard information in its possession. In addition, given the nature of the information at issue and the means by which Equifax collects it in furtherance of its billion-dollar business, the relationship between Plaintiffs and Equifax is sufficiently close and in privity to give rise to a duty owed to Plaintiffs by Equifax.

69. Equifax's duty required it to, among other things, design and employ cybersecurity systems, anti-hacking technologies, and intrusion detection and reporting systems sufficient to protect PII from unauthorized access. Duty further required Equifax to use systems and techniques sufficient promptly to alert Equifax to any such access and to enable Equifax to determine the extent of any breach or compromise.

70. Had Equifax designed, employed and maintained appropriate technological and other systems, PII would not have

been compromised – or, at a minimum, Equifax would have known sooner of the unauthorized access and would have been able to inform Plaintiffs and other Class members of the extent to which their PII was compromised.

71. Equifax breached its duties of care by, inter alia, failing to maintain appropriate systems and technologies to prevent unauthorized access; by failing to minimize the PII that any intrusion could compromise (for example, through cryptological countermeasures, or by discarding or disaggregating outdated data); and by failing to maintain systems and technologies capable of promptly notifying Equifax of a breach. It further breached its duties of care by failing to notify Plaintiffs and the Classes of the Data Breach sooner.

72. Equifax's breach of its duties provided the means for third parties including criminals to access, obtain and misuse Plaintiffs' and the Classes' PII without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and malfeasors intent on harming Plaintiffs.

73. Equifax's breaches of its duties directly and proximately injured Plaintiffs and the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to

which the breach puts their credit, reputation and finances at risk, and taking reasonable steps to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

74. As a result of Equifax's negligence, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT III

NEGLIGENCE PER SE

75. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

76. Plaintiffs assert this cause of action against Defendants on behalf of members of the Nationwide Class. In the event a nationwide class cannot be maintained on this cause of action, the claim is asserted by Atiles on behalf of the New York Class and by Solin on behalf of the New Jersey Class.

77. Equifax violated the FCRA.

78. Equifax also violated the Graham-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. (the "GLBA"), by (inter alia) failing to maintain and follow a written information security protocol with "administrative, technical and physical safeguards" commensurate

to the "size and complexity" of its business, the "nature and scope" of its activities, and the high "sensitivity of … consumer information at issue." 16 CFR § 314.3(a).

79. Defendants' violations of the FCRA, GLBA and/or state data breach notification laws (e.g., New York General Business Law § 899-aa; N.J.S.A. § 56:8-163(b)) constitute negligence per se.

80. Plaintiffs and the members of the Classes were foreseeable victims of Equifax's violations of its duties under statutes and regulations. The regulations and statutes violated by Equifax were enacted, promulgated or intended to protect Plaintiffs, Class members and other similarly situated consumers or members of the public.

81. Equifax's breach of its duties provided the means for third parties including criminals to access, obtain and misuse Plaintiffs' and the Classes' PII without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and malfeasors intent on harming Plaintiffs.

82. Equifax's breaches of its duties directly and proximately injured Plaintiffs and the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to

which the breach puts their credit, reputation and finances at risk, and taking reasonable steps to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

83. As a result of Equifax's negligence per se, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT IV

NEW YORK GENERAL BUSINESS LAW § 349

84. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

85. Plaintiff Atiles asserts this cause of action against Defendants on behalf of members of the New York Class.

86. New York General Business Law ("GBL") § 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York.

87. By reason of the conduct herein alleged, Equifax engaged in deceptive acts and practices within the meaning of the GBL.

88. Equifax stored PII of Plaintiffs and members of the New York Class in its databases. It used the PII in those databases for profit. Equifax represented to Plaintiffs and to members of the New York Class that their personal information and PII was secure and would remain private, and that it would be used and disclosed by Equifax only for lawful purposes.

89. Equifax violated GBL § 349 by falsely stating, for example, "[w]e limit access to your personal information;" that it employed "procedures and technology designed for th[e] purpose" of so limiting access; and that it had "reasonable physical, technical and procedural safeguards to help protect" consumers' personal information. Each of the foregoing false, deceptive and/or misleading statements was made by Equifax on its website, which was directed to consumers in New York.

90. Plaintiffs and members of the New York Class were entitled to and did reasonably rely on Equifax's statements that it would take appropriate measures to keep PII safe. Equifax did not disclose that Plaintiffs' personal information was vulnerable to hackers or that Equifax's data security measures were inadequate, outdated, or underfunded.

91. Equifax knew or should have known it did not employ reasonable measures that would have kept Plaintiffs' and other members of the New York Class's personal and financial

information secure, and that would have prevented loss or misuse of such personal and financial information.

92. Equifax's statements that it would secure and protect PII of Plaintiffs and members of the New York Class were facts upon which reasonable persons, including reasonable consumers in New York, could be expected to rely when deciding whether to conduct business with Equifax.

93. Equifax's misrepresentations and omissions were and are likely to mislead and did in fact materially mislead Plaintiffs and other reasonable consumers.

94. Equifax also violated its commitments to maintain the confidentiality and security of Plaintiffs' PII and members of the New York Class' PII, and failed to comply with its own policies and procedures, with applicable law and regulation, and with industry standards relating to data security.

95. Plaintiffs and other members of the New York Class suffered injury in fact and lost money or property as the result of Equifax's failure to secure their PII. As a direct result of Defendants' conduct, Plaintiffs and members of the New York Class have suffered or are in imminent risk of suffering forged credit applications and tax returns; improper or fraudulent charges to their credit and debit card accounts; and other similar harm. Moreover, Plaintiffs' and Class members' personal

information was stolen by and is in the possession of criminals who will use it for their own advantage (including commercial advantage) to the detriment of Plaintiffs and other Class members.

96. Plaintiffs' personal information was stolen by criminals because it has commercial value. The hacked information is of tangible value.

97. Plaintiffs and Class members have expended and will have to expend substantial sums to obtain credit freezes or additional identity theft protection services.

98. As a result of Equifax's violations of GBL § 349, Plaintiffs and the New York Class are entitled to damages, restitution and injunctive relief.

COUNT V

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT

99. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

100. Plaintiff Solin asserts this cause of action against Defendants on behalf of members of the New Jersey Class.

101. Under N.J.S.A. § 56:8-163(b), "[a]ny business or public entity that compiles or maintains computerized records

that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers … of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

102. Equifax is a business that compiles or maintains computerized records that include personal information on behalf of another business under N.J.S.A. § 56:8-163(b).

103. Plaintiffs' and the New Jersey Class members' PII, including names, addresses and SSNs, is personal information covered under N.J.S.A. § 56:8-163(b).

104. N.J.S.A. § 56:8-163(b) mandated that Equifax disclose the Data Breach to New Jersey consumers in a timely and accurate fashion upon Equifax's discovery of the Data Breach.

105. By failing to disclose the breach timely and accurately, Equifax violated N.J.S.A. § 56:8-163(b).

106. As a direct and proximate result of Equifax's violations of N.J.S.A. § 56:8-163(b), Plaintiffs and the New Jersey Class suffered damages as described above.

107. Plaintiffs and other members of the New Jersey Class suffered injury in fact and lost money or property as the result

of Equifax's violations of N.J.S.A. § 56:8-163(b). As a direct result of Defendants' conduct, Plaintiffs and members of the New Jersey Class have suffered or are in imminent risk of suffering forged credit applications and tax returns; improper or fraudulent charges to their credit and debit card accounts; and other similar harm. Moreover, Plaintiffs' and Class members' personal information was stolen by and is in the possession of criminals who will use it for their own advantage (including commercial advantage) to the detriment of Plaintiffs and other Class members.

108. As a result of Equifax's violations of N.J.S.A. § 56:8-163(b), Plaintiffs and the New Jersey Class seek relief under the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-19, including but not limited to treble damages in an amount to be proven at trial, attorney fees and costs, and injunctive relief.

COUNT VI

NEW JERSEY CONSUMER FRAUD ACT

109. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

110. Plaintiff Solin asserts this cause of action against Defendants on behalf of members of the New Jersey Class.

111. The New Jersey Consumer Fraud Act prohibits "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby …." N.J.S.A. § 56:8-2.

112. The New Jersey Consumer Fraud Act also prohibits "advertisement of merchandise as part of a plan or scheme not to sell the item or service so advertised." N.J.S.A. § 56:8-2.2.

113. In violation of N.J.S.A. § 56:8-2, while operating in New Jersey, Equifax engaged in unconscionable commercial practices, deception, misrepresentation and the knowing concealment, suppression and omission of material facts within intend that others rely on same, in connection with the sale and advertisement of services. Such conduct includes but is not limited to:

(a) Advertising and selling to Plaintiffs and to the Class a product and/or service designed to protect their PII, but then causing the theft of the same PII;

(b) Continuing to advertise identity theft protection services and consumer credit reporting and monitoring

services even after Equifax knew that it could not safely provide those services because its databases had been breached;

(c) Collecting, storing and using PII concerning consumers in aggregated online format over which consumers had no control and as to which Equifax failed to take reasonable or even basic measures to protect against unauthorized criminal access, which failures violated statutory and regulatory obligations and industry standards;

(d) Collecting, storing and using PII concerning consumers in aggregated online format over which consumers had no control and as to which Equifax failed to take reasonable or even basic measures to protect against unauthorized criminal access, which failures violated Equifax's own promises to the New Jersey public and to New Jersey consumers;

(e) Unreasonably delaying to give notice to New Jersey consumers after Equifax became aware of unauthorized access to those consumers' PII in its own database;

(f) Knowingly and fraudulently placing unreasonable and unlawful terms and conditions on consumers' efforts to obtain information from Equifax about the extent to which Equifax itself had compromised their PII;

(g) Knowingly and fraudulently coercing consumers into purchasing and/or enrolling in Equifax programs, products and services to redress injuries caused by Equifax's own conduct.

114. Equifax's misrepresentations and omissions were and are likely to mislead and did in fact materially mislead Plaintiffs and other reasonable consumers.

115. Equifax also violated its commitments to maintain the confidentiality and security of Plaintiffs' PII and members of the New Jersey Class' PII, and failed to comply with its own

policies and procedures, with applicable law and regulation, and with industry standards relating to data security.

116. Plaintiffs and other members of the New Jersey Class suffered injury in fact and lost money or property as the result of Equifax's failure to secure their PII. As a direct result of Defendants' conduct, Plaintiffs and members of the New Jersey Class have suffered or are in imminent risk of suffering forged credit applications and tax returns; improper or fraudulent charges to their credit and debit card accounts; and other similar harm. Moreover, Plaintiffs' and Class members' personal information was stolen by and is in the possession of criminals who will use it for their own advantage (including commercial advantage) to the detriment of Plaintiffs and other Class members.

117. Plaintiffs' personal information was stolen by criminals because it has commercial value. The hacked information is of tangible value.

118. The above unlawful and deceptive acts and practices by Equifax were immoral, unethical, unscrupulous and oppressive. These acts caused substantial injury to Plaintiffs that they could not reasonably avoid. The substantial injury outweighed any benefit to consumers or to competition.

119. Equifax knew or should have known that its computer systems and data security practices were inadequate to protect Plaintiffs' and the Class' PII; that the risk of a data breach (including the Data Breach) was high; and that its actions were unreasonable. Equifax's actions in engaging in the unfair practices and deceptive acts were knowing and willful.

120. As a result of Equifax's violations of New Jersey Consumer Fraud Act, Plaintiffs and the New Jersey Class seek relief under N.J.S.A. § 56:8-19, including but not limited to treble damages in an amount to be proven at trial, attorney fees and costs, and injunctive relief.

COUNT VII

UNJUST ENRICHMENT

121. Plaintiffs re-allege each and every allegation contained in the foregoing paragraphs with the same force and effect as if more fully set forth herein.

122. Plaintiffs assert this cause of action against Defendants on behalf of members of the Nationwide Class. In the event a nationwide class cannot be maintained on this cause of action, the claim is asserted by Atiles on behalf of the New York Class and by Solin on behalf of the New Jersey Class.

123. Defendants received payment to perform services that included protecting Plaintiffs' and Class members' PII. Defendants failed to perform those services but nevertheless retained Plaintiffs' and Class members' payments.

124. Defendants retained the benefit of said payments under circumstances which render it inequitable and unjust for Defendants to retain such benefits without paying for their value.

125. Plaintiffs and Class members are entitled to recover damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and in their capacity as representatives of the Nationwide Class, the New York Class, and the New Jersey Class, pray for relief against Defendants jointly and severally as follows:

A. An order certifying the proposed Classes under Fed. R. Civ. P. 23;

B. An order appointing Plaintiffs and their counsel to represent the Classes;

C. Declaratory judgment that the Defendant has engaged in the illegal conduct alleged;

D. An order that Defendant be permanently enjoined from its improper conduct;

E. A judgment awarding Plaintiff and the Classes restitution and disgorgement of all compensation obtained by Defendant inequitably and as a result of its wrongful conduct;

F. A judgment awarding Plaintiff and the Classes compensatory, statutory and punitive damages in an amount or amounts to be proven at trial;

G. Prejudgment and postjudgment interest;

H. Attorneys' fees and the costs and expenses of this action;

I. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: October 1, 2017
New York, NY

MULLEN P.C.

By: Wesley M. Mullen (WM1212)
200 Park Avenue, Ste. 1700
New York, NY 10166
wmullen@mullenpc.com
(646) 632-3718

Attorney for Plaintiffs José Atiles, Lauren Solin, and the Classes