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

TRACEY LORRAINE RUST, KIRBY PAYNE RUST, COREY STEDMAN, AVIVA YAGHOOBIA, PATRICK SHONTER KELLEY, KANDYCE CONNERLEY KELLEY, ROBERT CLARK, BRANDON PARR, LAURA ROUDABUSH, and JEFF ROUDABUSH individually and on behalf of all others similarly situated, Plaintiffs, v. EQUIFAX, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiffs Tracey Lorraine Rust, Kirby Payne Rust, Corey Stedman, Aviva Yaghoobia, Patrick Shonter Kelley, Kandyce Connerley Kelley, Robert Clark, Brandon Parr, Jeff Roudabush, and Laura Roudabush (collectively the "Plaintiffs"), individually and on behalf of all others similarly situated persons, allege the following against Equifax, Inc. ("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:

NATURE OF THE CASE

1. This is a consumer class action against Defendant for its failure to secure and safeguard the sensitive personal information of approximately 143 million Americans, including, but not limited to, their credit card numbers ("Payment Card Data" or "PCD"), names, Social Security numbers, driver's license numbers, birth dates, and addresses ("Personally Identifiable Information" or "PII").

2. On September 7, 2017, Defendant announced that a data breach at the company between mid-May through July 2017 may have affected approximately 143 million Americans, exposing their PCD and PII to criminals who were able to gain access to the PCD and PII by exploiting an application vulnerability to gain access.[1]

3. This private PCD and PII was compromised due to Defendant's acts and omissions and its failure to properly safeguard the PCD and PII.

[1] https://www.equifaxsecurity2017.com/ (last visited on September 11, 2017).

4. In addition to Defendant's failure to prevent the data breach, Defendant also failed to detect the breach for nearly three months, finally detecting the beach on July 29, 2017.

5. Despite becoming of aware of this massive data breach in July of 2017, Defendant withheld notice of the beach from Plaintiffs and other individuals until September of 2017 in blatant disregard of its duties, and without any plausible justification.

6. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems and the PCD and PII were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to detect the breach for nearly three months, and failing to disclose the breach in a timely manner.

7. Had Defendant implemented and maintained adequate safeguards to protect the PCD and PII and deter the hackers, and detect the breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented.

8. Furthermore, had Defendant disclosed the breach in a timely manner, the impact of the breach on Plaintiff and other Class members may have been reduced.

9. As a result of the Equifax data breach, the PCD and PII of the Plaintiffs and other Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and the other Class members as a direct result of the data breach include:

a. unauthorized charges on their payment cards;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their payment card accounts because their account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Equifax data breach including, but not limited to, foregoing cash back and other rewards;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach,

including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax data breach;

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

h. damages to and diminution in value of their PCD and PII; and

i. loss of Plaintiffs' and Class member's privacy; and

j. continued risk to their PCD and PII which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data in its possession.

10. The injuries to the Plaintiffs and members of the Classes were directly and proximately caused by Defendant's failure to update its security systems, and/or implement or maintain adequate data security measures for the PCD and PII. Defendant failed to take steps to employ adequate security measures despite recent, well-publicized data breaches at Equifax itself as well as and other credit bureaus including Experian PLC. In May 2017, KrebsOnSecurity reported that hackers exploited lax security at Defendant's TALX payroll division, which provides online

payroll, HR, and tax services. In 2015, a data breach at Experian PLC jeopardized the sensitive personal information of at least 15 million consumers.

11. Plaintiffs retain a significant interest in ensuring that their PCD and PII, which remains in the possession of Defendant, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PCD and PII was stolen as a result of the Equifax data breach. Plaintiffs assert claims against Defendant for violations of the Fair Credit Reporting Act, 15 U.S.C. 1681, *et seq.* ("FCRA") and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* (the "UCL"), as well as negligence, negligence per se, unjust enrichment, and declaratory relief.

12. Plaintiffs bring this class action on behalf of a Nationwide Class, a Georgia Subclass, a New York Subclass, a California Subclass, a Florida Subclass, a New Jersey Subclass, an Ohio Subclass, and a Virginia Subclass (collectively referred to as the "Classes").[2]

13. Plaintiffs, on behalf of the Classes, seek to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the data breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

---

[2] Classes defined further, *infra*, in paragraphs 64-71.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

15. This Court has personal jurisdiction over Defendant because Defendant is incorporated and maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant therefore intentionally avails itself of this jurisdiction.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District.

PARTIES

17. Plaintiffs Tracey Lorraine Rust and Kirby Payne Rust are residents of Atlanta Georgia, and were residents of Georgia during the period of the Equifax data breach. Defendant has confirmed that the Rust Plaintiffs' personal information was impacted by the Equifax data breach.

18. Plaintiff Corey Stedman is resident of White Plains, New York, and was a New York residents during the period of the Equifax data breach. Defendant

has confirmed that Plaintiff Stedman's personal information was impacted by the Equifax data breach.

19. Plaintiff Aviva Yaghoobia is a resident of Los Angeles, California and was a resident of California during the period of the Equifax data breach. Defendant has confirmed that Plaintiff Yaghoobia's personal information was impacted by the Equifax data breach.

20. Plaintiffs Patrick Shonter Kelley and Kandyce Connerley Kelley are residents of Naples, Florida and were residents of Florida during the period of the Equifax data breach. Defendant has confirmed that the Kelley Plaintiffs' personal information was impacted by the Equifax data breach. As a result of the Equifax data breach, the Kelley Plaintiffs incurred suspicious charges on their credit card accounts and as a result, had to cancel their credit card. As a result of canceling her credit card, Plaintiff Kandyce Connerley Kelley lost the ability to earn rewards points that she would have otherwise received if her identity had not been stolen.

21. Plaintiff Robert Clark is a resident of Lyndhurst, New Jersey, and was a resident of New Jersey during the period of the Equifax data breach. Defendant has confirmed that Plaintiff Clark's personal information was impacted by the Equifax data breach.

22. Plaintiff Brandon Parr is a resident of Sylvania, Ohio, and was a resident of Ohio during the period of the Equifax data breach. Defendant has confirmed that Plaintiff Parr's personal information was impacted by the Equifax data breach.

23. Plaintiffs Jeff and Laura Roudabush are residents of Leesburg, Virginia, and were residents of Virginia during the period of the Equifax data breach. Defendant has confirmed that Plaintiff Camp's personal information was impacted by the Equifax data breach.

24. Each of the Plaintiffs suffered actual injury from having his or her PCD and PII compromised and stolen in and as a result of the Equifax data breach.

25. Each of the Plaintiffs suffered actual injury in the form of damages to and diminution in the value of his or her PII and PCD – a form of intangible property in the possession of Defendant that was compromised in and as a result of the Equifax data breach.

26. Each of the Plaintiffs has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his or her PCD and PII being placed in the hands of criminals who have already misused such information stolen in the Equifax data breach via sale of Plaintiffs' and Class members' PII and PCD on the Internet black market. Plaintiffs

also have a continuing interest in ensuring that their private information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

27. Defendant Equifax, Inc. is a Georgia corporation with its principal place of business located at 1550 Peachtree Street, N.W. Atlanta, Georgia 30309. Defendant is a credit reporting agency and is considered to be one of the three largest American credit agencies. During the period of the data breach, Defendant was in the possession of Plaintiff and other Class members' PII and PCD. Defendant allowed a massive data breach of the PII and PCD it collected and maintained to occur, effecting approximately 143 million Americans, which is the subject of this Complaint.

STATEMENT OF FACTS

1. Background

28. Defendant is a consumer credit reporting agency which regularly engages in the practice of assembling and/or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties on a nationwide basis. Defendant gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

29. In the process of providing said credit reporting services and other services, Defendant collects and stores massive amounts of PCD and PII on its servers and utilizes this information to maximize profits.

30. The PCD and PII that Defendant collects and stores is an extremely valuable commodity. A "cyber black-market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. The PII and PCD is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

31. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[3]

32. Furthermore, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's

[3] https://www.consumer.ftc.gov/articles/0271-warning-signsidentity-theft (last visited September 11, 2017).

information to obtain a fraudulent refund. Some of this activity may not come to light for years.

33. At all relevant times, Defendant was well-aware, or reasonably should have been aware, of the importance of safeguarding the PCD and PII of Plaintiffs and other Class members in its possession, and of the foreseeable consequences that would occur if its data security systems were breached, specifically, including the significant costs that would be imposed as a result of a breach.

34. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that hackers had been targeting credit reporting agencies and other companies many years. Notably, in May 2017, KrebsOnSecurity reported that hackers exploited lax security at Defendant's own TALX payroll division, which provides online payroll, HR, and tax services.[4] Furthermore, in 2015, a data breach at Experian PLC jeopardized the sensitive personal information of at least 15 million consumers. Other notable data breaches in the past few years include retailer such as Home Depot and Target and restaurant chains including Arby's, P.F. Chang's, and Wendy's.

[4] https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/ (last visited on September 11, 2017).

35. Furthermore, the FTC Act imposes a duty on Defendant to use adequate care to protect the sensitive PCD and PII in its possession:

36. *FTC Act*:

a. Pursuant to the Federal Trade Commission ("FTC"), the failure to employ reasonable and adequate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45.

b. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses, noting businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for

large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

c. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[5]

d. The FTC has issued orders against businesses that failed to employ reasonable measures to secure PCD and PII. These orders provide further guidance to businesses with regard to their data security obligations.

2. The Equifax Data Breach

37. On September 7, 2017, Defendant reported that a data breach at the company between mid-May through July 2017 may have affected approximately 143 million U.S. consumers, including approximately 209,000 credit card numbers ("PCD"), names, Social Security numbers, driver's license numbers, birth dates, and addresses ("PII").[6]

[5] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited on September 11, 2017).

[6] https://www.equifaxsecurity2017.com/ (last visited on September 11, 2017).

38. Defendant reported that the PCD and PII was accessed by criminals who were able to gain access by exploiting an application vulnerability.

39. Upon information and belief, Defendant failed to encrypt or maintain its encryption keys on stored PII and PCD.

40. Defendant has not fully disclosed the extent of the breach or its impact on those whose PCI and PCD was compromised. Defendant has not disclosed what other private personal and financial it collects or stores were stolen or accessed in the breach, instead providing solely a sample set of categories which may have been disclosed. Without a detailed disclosure, Plaintiffs and other Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

41. This private information was compromised due to Defendant's acts and omissions and its failure to properly protect the PII and PCD, despite being aware of the recent data breaches impacting itself, other credit reporting agencies, and various other businesses.

42. In addition to Defendant's failure to prevent the data breach, Defendant also failed to detect the breach for nearly three months after it had started. According to Defendant, it detected the data breach on July 29, 2017.[7]

[7] https://www.equifaxsecurity2017.com/ (last visited on September 11, 2017).

43. Furthermore, Defendant failed to disclosed the occurrence of the breach to Plaintiff and other Class members until September 2017, more than one month after learning of the incident.

44. The breach occurred because Defendant failed to implement adequate data security measures to protect the PCI and PCD, and failed to implement and maintain adequate systems to detect and prevent the breach and resulting harm that it has caused.

45. Had Defendant implemented and maintained adequate safeguards to protect the PII and PCD, deter the hackers, and detect the data breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented or mitigated.

3. The Equifax Data Breach Caused Harm And Will Result In Additional Harm To Plaintiffs And Other Class Members

46. The Equifax data breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiffs' and Class members' PII and PCD from unauthorized access, use, and disclosure, as required by state and federal regulations and statutory law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PCD and PII, and

its failure to protect against reasonably foreseeable threats to the security or integrity of such information.

47. As a result of the breach, the PCD and PII of Plaintiffs and Class members has been exposed to criminals for misuse.

48. The ramifications of Defendant's failure to keep Plaintiffs' and Class members' PCD and PII are severe.

49. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[9]

50. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year."[10]

51. Identity thieves can use personal information such as that pertaining to the Class, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of

---

8 17 C.F.R § 248.201 (2013).

9 *Id.*

10 http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identity-theft-victim-every-2-seconds-last-year/ (last visited September 11, 2017).

government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. This activity may not come to light for years.

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

53. Thieves are already using the PCD and PII stolen from Defendant to commit actual fraud, as evidenced by the unauthorized charges on the Kelley Plaintiffs' credit card accounts, as alleged herein.

54. The injuries suffered by Plaintiffs and the proposed Classes (and which they will continue to suffer) as a direct result of the Equifax data breach include, but are not limited, to those listed in Paragraph 9.

55. In addition, many victims spent or will spend substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Resetting automatic billing instructions; and

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments;

i. Paying fees to implement credit freezes to attempt to mitigate damages; and

j. Transaction costs for delayed or missed business opportunities because of the necessity of implementing credit freezes.

56. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PCD and PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[11]

[11] Government Accounting Office. *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full*

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

57. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning that Plaintiff and other Class members could be at risk of fraud and identity theft for years into the future. Given the breadth of Defendant's market share, Plaintiff and other Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them, and the resulting loss of use of their credit and access to funds whether or not such charges are ultimately reimbursed by the credit card companies.

58. Despite acknowledging the repercussions from its wrongful actions and inaction and the resulting breach, Defendant has not offered to cover any of the damages sustained by Plaintiffs or Class members, as well as any future damages and costs they will incur. Furthermore, the cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Defendant's actions

---

Extent Is Unknown, 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited September 11, 2017).

have created for Plaintiffs and Class members, is ascertainable and is a determination appropriate for the trier of fact.

59. While the PII and PCD of Plaintiffs and Class members has been stolen, Defendant continues to maintain and store PII and PCD, including Plaintiffs' and other Class members'. Particularly because Defendant has demonstrated an inability to prevent a breach (twice), stop it from continuing even after being detected, or disclosing it in a timely manner, Plaintiffs and members of the Class have an undeniable interest in insuring that their PII and PCD is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

60. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), Plaintiffs seek to certify a class of all natural persons residing in the United States whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "Nationwide Class").

61. The Rust Plaintiffs also seek to certify a class of all natural persons residing in Georgia whose PCI or PCD was acquired or accessed by unauthorized

persons in the data breach announced by Defendant on September 7, 2017 (the "Georgia Subclass").

62. Plaintiff Stedman also seeks to certify a class of all natural persons residing in New York whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "New York Subclass").

63. Plaintiff Yaghoobia also seeks to certify a class of all natural persons residing in California whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "California Subclass").

64. The Kelley Plaintiffs also seek to certify a class of all natural persons residing in Florida whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "Florida Subclass").

65. Plaintiff Clark also seek to certify a class of all natural persons residing in New Jersey whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "New Jersey Subclass").

66. Plaintiff Parr also seeks to certify a class of all natural persons residing in Ohio whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "Ohio Subclass").

67. The Roudabush Plaintiffs also seek to certify a class of all natural persons residing in Virginia whose PCI or PCD was acquired or accessed by unauthorized persons in the data breach announced by Defendant on September 7, 2017 (the "Virginia Subclass").

68. Excluded from each of the Classes are Defendant and any of its parents or subsidiaries, any entities in which they have 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.

69. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

70. Each of the proposed Classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3):

71. **Numerosity.** According to Defendants, over 140 million Americans were impacted by the data breach. In addition, at least 209,000 credit card numbers

were stolen or accessed as a result of the breach. While the precise number of Class members has not yet been determined, the massive size of the data breach indicates that joinder of each member would be impracticable.

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

a. Whether Defendant had a duty to protect the PCD and PII;

b. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

c. Whether Defendant's conduct constitutes deceptive or unfair trade practices under the various consumer protection statutes.

d. Whether Defendant's conduct constitutes a violation of the Fair Credit Reporting Act.

e. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PCD and PII of Plaintiffs and Class members;

f. whether Defendant's breaches of its legal duties caused Plaintiffs and the Class members to suffer damages;

g. whether Plaintiffs and Class members are entitled to recover damages; and

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

73. **Typicality.** Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and Class members were injured through Defendant's uniform misconduct or failure to act, and their legal claims arise from the same core practices employed or omitted by Defendant.

74. **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 is experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive data breach cases.

75. **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 Defendant. 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.

76. This lawsuit is maintainable as a class action under Federal Rule of Civil Procedure 23(b)(2) because Defendant have acted or refused to act on grounds that are generally applicable to the class members, thereby making final injunctive relief appropriate with respect to all Classes.

77. This lawsuit is also maintainable as a class action under Federal Rule of Civil Procedure 23(b)(3) because the questions of law and fact common to the members of the Classes predominate over any questions that affect only individual members, and because the class action mechanism is superior to other available methods for the fair and efficient adjudication of the controversy.

78. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to information regarding those affected by the breach, the time period of the breach, as well as the addresses and other contact information for members of the Classes, which can be used for providing notice to the Class members.

COUNT I
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")
(*On Behalf of the Nationwide Class*)

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

80. Plaintiffs bring this Count on behalf of themselves and all other members of the Nationwide Class against Defendant.

81. Plaintiffs and the Nationwide Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

82. The FCRA defines a "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . ." 15 U.S.C. § 1681a(f).

83. The FRCA defines a "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness [creditworthiness], credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be

used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [15 USCS § 1681b]." 15 U.S.C. § 1681a(d)(1).

84. Defendant is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

85. The compromised PCD and PII were consumer reports under the FCRA because they information in a communication bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

86. As a consumer reporting agency, Defendant is required under the FCRA to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

87. 15 U.S.C. § 1681b limits the ability of consumer reporting agencies to furnish consumer reports for specific enumerated purposes and no others. None of

the specific purposes listed in 15 U.S.C. § 1681b allow credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the information here.

88. Defendant furnished Plaintiffs' and the Nationwide Class members' consumer reports by disclosing the PCD and PII contained within consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports to obtain the PCD and PII; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

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

90. Defendant willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

91. Defendant also acted willfully and recklessly because it knew about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See*, *e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary on the Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Defendant obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows about these requirements. Despite knowing of these legal obligations, Defendant acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the Nationwide Class of their rights under the FCRA.

92. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

93. Plaintiffs and the Nationwide Class members have been damaged by Defendant's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not

more than $1,000." 15 U.S.C. § 1681n(a)(1)(A). Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2), (3).

COUNT II
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(*On Behalf of the Nationwide Class*)

94. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

95. Plaintiffs bring this Count on behalf of themselves and all other members of the Nationwide Class against Defendant.

96. Defendant was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes specified under 15 U.S.C. § 1681b.

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

the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite the fact that Defendant knew or should have known of these legal obligations, Defendant acted negligently in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

98. Defendant's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PCD and PII purposes not permissible under the FCRA.

99. Plaintiffs and the Nationwide Class members have been damaged by Defendant's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1). Plaintiffs and the Nationwide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III
NEGLIGENCE
(*On Behalf of the Nationwide Class*)

100. Plaintiff incorporate by reference all paragraphs above as if fully set forth herein.

101. Plaintiffs bring this Count on behalf of themselves and members of the Nationwide Class against Defendant.

102. Upon accepting and storing the PCD and PII of Plaintiffs and the Nationwide Class members in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Nationwide Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the PCD and PII of consumers was private and confidential and should be protected as private and confidential.

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

104. Defendant owed numerous other duties to Plaintiffs and to members of the Nationwide Class members, including the following:

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

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

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

105. Defendant breached its duty to Plaintiffs and the Nationwide Class members to adequately protect and safeguard PCD and PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PCD and PII. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the PCD and PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted unknown hackers to gather the PCD and PII of Plaintiffs and the Nationwide Class members, misuse the PCD and PII, and intentionally disclose such information to others without the consent of Plaintiffs and the Nationwide Class members.

106. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and PCD, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-

publicized data breaches, including the breach at Experian and its own prior data breach.

107. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and the Nationwide Class members' PCD and PII.

108. Defendant breached its duties to Plaintiffs and the Nationwide Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PCD and PII of Plaintiffs and the Nationwide Class members.

109. Because Defendant knew that a breach of its systems would damage millions of individuals, including Plaintiffs and the Nationwide Class members, Defendant had a duty to adequately protect their data systems and the PCD and PII contained thereon.

110. Defendant had a special relationship with Plaintiffs and the Nationwide Class members. Plaintiffs' and the Nationwide Class members' willingness to entrust Defendant with their PCD and PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PCD and PII it stored on them from security breaches.

111. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Nationwide Class members and their PCD and PII. Defendant's misconduct included failing to:

a. secure its systems, despite knowing their vulnerabilities;

b. comply with industry standard security practices;

c. implement adequate system and event monitoring; and

d. implement the systems, policies, and procedures necessary to prevent this type of data breach.

112. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and the Class members' PCD and PII and promptly notify them about the data breach.

113. Defendant breached its duties to Plaintiffs and the Nationwide Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PCD and PII of Plaintiffs and the Nationwide Class members;

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

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and the Nationwide Class members' PCD and PII both before and after learning of the data breach;

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

e. by failing to timely detect that Plaintiffs' and the Class members' PCD and PII had been improperly acquired or accessed.

114. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PCD and PII of Plaintiffs and the Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PCD and PII of Plaintiffs and the Class members during the time it was within Defendant's possession or control.

115. Upon information and belief, Defendant improperly and inadequately safeguarded the PCD and PII of Plaintiffs and the Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect sensitive

PCD and PII of Plaintiffs and the Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the PCD and PII of Plaintiffs and the Class members.

116. Defendant's conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect PCD and PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to the PCD and PII of Plaintiffs and the Class members.

117. Furthermore, Defendant was negligent in failing to detect the breach for nearly three months, as well as failing to timely disclose the occurrence of the breach in a timely fashion.

118. Neither Plaintiffs nor the other Class members contributed to the data breach and subsequent misuse of their PCD and PII as described in this Complaint.

119. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members suffered damages including, but not limited to those alleged in Paragraph 9.

COUNT IV
NEGLIGENCE PER SE
(*On Behalf of the Nationwide Class*)

120. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

121. Plaintiffs bring this Count on behalf of themselves and members of the Nationwide Class against Defendant.

122. Under the FCRA, 15 U.S.C. §§ 1681e, Defendant is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

123. Defendant failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

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

125. Defendant was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards, including:

a. to insure the security and confidentiality of customer records and information;

b. to protect against any anticipated threats or hazards to the security or integrity of such records; and

c. to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. 15 U.S.C. § 6801(b).

126. In order to satisfy its obligations under the GLBA, Defendant was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

127. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Defendant had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

128. Further, when Defendant became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.*

129. Defendant violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Defendant's:

a. failure to implement and maintain adequate data security practices to safeguard Plaintiffs and the Class members' PCD and PII;

b. failure to detect the Data Breach in a timely manner; and

c. failure to disclose that Equifax's data security practices were inadequate to safeguard Plaintiffs' and the Class members' PCD and PII.

130. Defendant also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems."

131. Plaintiffs and the Class members were foreseeable victims of Defendant's violation of the GLBA. Defendant knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems would cause damages to Plaintiffs and the Class members.

132. Defendant's failure to comply with the applicable laws and regulations, including the FCRA and the GLBA, constitutes negligence *per se*.

133. But for Defendant's violation of the applicable laws and regulations, Plaintiffs' and the Class members' PCD and PII would not have been accessed by unauthorized individuals.

134. As a direct and proximate result of Defendant's violation of laws and regulations, Plaintiffs and the Class members suffered damages including, but not limited to those alleged in Paragraph 9.

COUNT V
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
(*On Behalf of the California Subclass*)

135. Plaintiff Yaghoobia incorporates by reference all paragraphs above as if fully set forth herein.

136. Plaintiff Yaghoobia brings this Count on behalf of herself and members of the California Subclass against Defendant.

137. California Business & Professions Code § 17200 prohibits any "unlawful…business act or practice." For the reasons discussed above, Defendant violated and continues to violate California's Unfair Competition Law, California Business & Professions Code § 17200 *et seq.*, by engaging in the above-described unlawful acts and practices.

138. Defendant's unfair and fraudulent acts and practices include but are not limited to the following:

a. failing to enact adequate privacy and security measures, in California, to protect the California Subclass members' PCD and PII from unauthorized disclosure, release, data breaches, and theft, in violation of industry standards and best practices, which was a direct and proximate cause of the data breach;

b. failing to take proper action, in California, following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. failing to maintain reasonable security;

d. failing to timely detect the data breach; and

e. failing to timely disclose the occurrence of the data breach to Plaintiff and California Subclass members.

139. Defendant's acts and practices also constitute "unlawful" business acts and practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as described fully above), the GLBA, 15 U.S.C. § 6801 *et seq.* (as described fully above), and common law (as described fully above).

140. There were reasonably available alternatives to further Defendant's legitimate business interests, including complying with industry standards and using best practices to protect the California Subclass members' PCD and PII, other than Defendant's wrongful conduct described herein.

141. Defendant knew or should have known that its data security practices and infrastructure were inadequate to safeguard the California Subclass members' PCD and PII, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above named unlawful practices was negligent, knowing and willful, and/or wanton and reckless with respect to California Subclass members' rights.

142. On information and belief, Defendant's unlawful and unfair business practices, except as otherwise indicated herein, continue to this day and are ongoing.

143. As a direct and/or proximate result of Defendant's unlawful practices, the California Subclass has suffered damages including, but not limited to those listed in paragraph 9.

144. Under Business and Professions Code § 17200 *et seq.*, the California Subclass seeks restitution of money or property that Defendant may have acquired by means of Defendant's unlawful and unfair business practices (to be proven at trial), restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices (to be proven at trial), declaratory relief, and attorney's fees and costs (including those allowed by Cal. Code Civil Pro. §1021.5).

COUNT VI
DECLARATORY RELIEF
(*On Behalf of the Nationwide Class*)

145. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

146. Plaintiffs bring this Count on behalf of themselves and members of the Nationwide Class against Defendant.

147. As previously alleged, Defendant was required to provide adequate security measures for Plaintiffs' and Nationwide Class members' PCD and PII it collected. Defendant owes duties of care to Plaintiffs and the Nationwide Class members that require it to adequately secure PCD and PII.

148. Defendant still possesses the PCD and PII of Plaintiffs and the Nationwide Class members.

149. Defendant has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

150. Accordingly, Defendant has not satisfied its legal duties to Plaintiffs and the Nationwide Class members. In fact, now that Defendant's lax approach towards data security has become public, the PCD and PII in its possession is more vulnerable than it was previously.

151. Actual harm has arisen in the wake of Defendant's data breach regarding Defendant's duties of care to provide adequate data security measures to Plaintiffs and the Nationwide Class members.

152. Plaintiffs, therefore, seek a declaration that (a) Defendant's existing data security measures do not comply with its duties of care, and (b) in order to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's

systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PCD and PII by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. purging, deleting, and destroying in a reasonable secure manner PCD and PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks; and

g. routinely and continually conducting 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.

COUNT VII
UNJUST ENRICHMENT

153. Plaintiffs restate and reallege Paragraphs 1 through 152 as if fully set forth here.

154. Plaintiffs and Class members conferred a monetary benefit on Defendant. Specifically, they allowed Defendant to collect and possess their most sensitive and private personal information (PCD and PII). In exchange, Plaintiffs and Class members were entitled to have Defendant protect their PCD and PII with adequate data security.

155. Defendant knew that Plaintiffs and Class members conferred a benefit on Defendant and accepted and has retained that benefit. Defendant profited from the use of the PCD and PII of Plaintiffs and Class members for business purposes.

156. Defendant failed to secure the PCD and PII of Plaintiffs and Class members and, therefore, did not provide full compensation for the benefit the Plaintiffs and Class members provided.

157. Defendant acquired the PCD and PII through inequitable means as it failed to disclose the inadequate security practices in place, as previously alleged.

158. If Plaintiffs and Class members knew that Defendant would not secure their PCD and PII using adequate security, they would not have allowed Defendant access to that information.

159. Plaintiffs and Class members have no adequate remedy at law.

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

161. Defendant 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.

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 appoints the Counsel representing Plaintiffs as Class counsel;

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

C. on behalf of Plaintiffs and the Classes, enters an injunction against Defendant, and requiring it to implement and maintain adequate security measures, including the measures specified above to ensure the

protection of Plaintiffs' and Class members' information, which remains in the possession of Defendant;

D. orders Defendant to pay the costs involved in notifying the Class members about the judgment any administering the claims process;

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

F. 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.

Dated: September 11, 2017

Respectfully submitted,

/s Robert W. Killorin
FARUQI & FARUQI, LLP
Robert W. Killorin
Ga. Bar No. 417775
Attorney at Law
3975 Roswell Rd.
Suite A
Atlanta, GA 30342
Telephone: (404) 847-0617
Facsimile: (404) 506-9534
Email: rkillorin@faruqilaw.com

Timothy J. Peter
101 Greenwood Avenue, Suite 600
Jenkintown, PA 19046
Telephone: (215) 277-5770
Facsimile: (215) 277-5771
Email: tpeter@faruqilaw.com

Pro hac vice application forthcoming

James M. Wilson, Jr.
685 Third Ave., 26th Floor
New York, NY 10017
Telephone: (212) 983-9330
Facsimile: (212) 983-9331
Email: jwilson@faruqilaw.com

Pro hac vice application forthcoming

Attorneys for the Plaintiffs

JS44 (Rev. 11/16 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

TRACEY LORRAINE RUST, KIRBY PAYNE RUST, COREY STEDMAN, AVIVA YAGHOOBIA, PATRICK SHONTER KELLEY, KANDYCE CONNERLEY KELLEY, ROBERT CLARK, BRANDON PARR, LAURA ROUDABUSH, and JEFF ROUDABUSH individually and on behalf of all others similarly situated

DEFENDANT(S)

Equifax, Inc.

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Fulton County
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton County
(IN U.S. PLAINTIFF CASES ONLY)

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

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Robert W. Killorin, rkillorin@faruqilaw.com
FARUQI & FARUQI, LLP
3975 Roswell Rd, Suite A
Atlanta, GA 30342
(404) 847-0617

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)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☐ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☐ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

- ☑ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Class Action Fairness Act, 28 U.S.C. § 1332(d)(2); Willful Violation of The Fair Credit Reporting Act ("FCRA"); Negligent Violation of FCRA; Negligence; Negligence Per Se; Violation of California UCL; Declaratory Relief; Violation of Fed. Rule of Civ. P. 23;

(IF COMPLEX, CHECK REASON BELOW)

- ☑ 1. Unusually large number of parties.
- ☑ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☑ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☒ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** < 5,000,000.00

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

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE William S. Duffey, Jr. **DOCKET NO.** 1:17-cv-03422-WSD

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☑ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

/s Robert W. Killorin — **SIGNATURE OF ATTORNEY OF RECORD**

September 11, 2017 — **DATE**