

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

BAKKEN, Keri; and SANCHEZ,  
Gustavo Carlo

Plaintiffs,

vs.

EQUIFAX, INC.,

Defendant.

Civil Action No.:

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiffs Keri Bakken and Gustavo Carlo Sanchez (hereinafter, collectively, “Plaintiffs”), individually and on behalf of the Classes defined below, allege the following against Equifax, Inc. (“Equifax”) 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. Plaintiffs bring this class action case against Defendant Equifax for failing to protect consumers’ personally identifiable information (“PII”) which Equifax collected from various sources in the course of its operation as a consumer

credit reporting agency, and for failing to provide timely, accurate and adequate notice to Consumer Plaintiffs and other Class members that their PII had been stolen, the extent of the PII stolen and precisely what types of information were stolen.

2. Equifax has acknowledged a cybersecurity breach of their data storages (“Data Breach”) potentially impacting approximately 143 million U.S. consumers. Equifax has stated unauthorized persons exploited a U.S. website application vulnerability to gain access to the protected information. It claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The data accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Equifax has also admitted that the unauthorized users accessed credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers.

3. Equifax has acknowledged that it discovered the unauthorized access on July 29, 2017, but has failed to inform the public why it delayed notification of the Data Breach to consumers.

4. The PII of Plaintiffs and the class of consumers they seek to represent was compromised due to Equifax's acts and omissions and their failure to properly protect the PII.

5. Equifax could have prevented this Data Breach. Such unauthorized attacks against data storehouses are known. Data breaches at other companies, including one of its major competitors, Experian have occurred.

6. The Data Breach was the predictable result of Equifax's inadequate approach to data security and the protection of the PII that it obtained in its course of business.

7. Equifax disregarded the rights of Plaintiffs and Class members by deliberately, recklessly, or negligently declining to take adequate and reasonable measures to protect its data systems, failing to disclose to its customers the material fact that it did not have adequate precautions to safeguard PII, failing to take reasonable steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach in a timely manner.

8. Because of the Equifax Data Breach, the Plaintiff and Class member's PII has been exposed to criminals for misuse. The injuries suffered, or likely to be suffered, by Plaintiffs and Class members, as a direct result of the Equifax Data Breach include:

- a. unauthorized use of their PII;
- 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 PII;
- 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 or the enjoyment of one's life 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, purchasing credit monitoring and identity theft protection services, 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 identity theft posed by their 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 PII entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and

i. the loss of Plaintiff's and Class members' privacy.

9. Equifax's failure to keep adequate security protections for PII directly and proximately caused the Plaintiffs' and Class members' injuries.

10. Plaintiffs still hold a significant interest in ensuring that their PII, which remains in the possession of Equifax is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PII was stolen because of the Equifax Data Breach.

11. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

Plaintiffs seek numerous remedies, including among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses and expenses, other compensatory damages, further and more robust credit monitoring services with accompanying

identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

### **JURIDICTION AND VENUE**

12. 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. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Equifax.

13. This Court has personal jurisdiction over Equifax because Equifax maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Equifax intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Georgia.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

**PARTIES**

15. Plaintiff Keri Bakken is a resident of the state of Wisconsin. Plaintiff is a victim of the Data Breach. Upon notice of her PII being stolen, Plaintiff Bakken has undertaken the cost of employing identity theft protection services for her credit history accounts. This is a cost she will be subjected to for the rest of her life.

16. Plaintiff Gustavo Carlo Sanchez is a resident of the state of Florida. Plaintiff is also a victim of the Data Breach. As a consequence of the Data Breach, Plaintiff will require heightened, perpetual monitoring of credit accounts and records at multiple credit agencies. This will require either an investment of personal time or financial cost to ensure that unauthorized uses of Plaintiff's identity and information are not recorded and assessed against Plaintiff.

17. Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office address identified above.

**STATEMENT OF FACTS**

18. Equifax is one of three nationwide credit-reporting companies that track and rates the financial history of U.S. consumers. The companies are supplied

with data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history. All this information, and more factors into credit scores.

19. Unlike other data breaches, not all of the people affected by the Equifax breach may be aware that they are customers of the company. Equifax 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.

20. According to Equifax's report on September 7, 2017, the breach was discovered on July 29th. The hackers gained access by "[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to obtain "certain files."

21. The hackers obtained a wide variety of personal data: names, dates of birth, Social Security numbers and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.



22. This type of data may be used by ill-willed individuals to target the victims with future fraudulent activity.

23. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII – a form of intangible property that Plaintiffs entrusted to Equifax and that was compromised in and as a result of the Equifax Data Breach.

24. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

25. Plaintiffs have a continuing interest in ensuring that their private information, which continues to remain in the possession of Equifax, is protected and safeguarded from future breaches.

26. At all relevant times, Equifax was aware, or reasonably should have been aware, that the PII collected, maintained and stored is highly sensitive, frequently targeted by hostile attacks, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

27. PII is commonly known as highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate

entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

28. PII is a valuable commodity because it contains not only payment card numbers but information that may lead to other fraudulent acquisitions of money, property, or other stolen information. A “cyber black market” exists in which criminals openly offer stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is highly sought after 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.

29. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant’s data systems; otherwise, they would not aggressively seek or pay for it. For example, in “one of 2013’s largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users.”

30. At all relevant times, Equifax knew, or reasonably should have known, of the imperative of protecting PII and of the foreseeable consequences

that would occur if its data security system was breached, including, specifically, the significant costs, risks, and losses that would be imposed on individuals as a result of a breach.

31. Equifax was, or should have been, fully aware of the high volume of people whose PII it collected, and thus, the significant number of individuals who would be at risk by a breach of Equifax's systems.

32. Equifax's approach to maintaining the privacy and security of the PII of Plaintiffs and Class members was poor, uninformed, reckless, or at the very least, negligent.

33. Identity thieves can use PII to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

34. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. Identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

35. There may also be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

36. Plaintiffs and Class members now require years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

37. Equifax failed to adequately protect PII, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

38. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

39. If Equifax had remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the access of its customers' PII.

40. As a direct and proximate result of Equifax's wrongful actions and inaction, Plaintiffs and Class members are affected by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

41. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. theft of their personal and financial information;
- b. unauthorized charges on their debit and credit card accounts;
- c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the black market;
- d. the untimely and inadequate notification of the Data Breach;
- e. the improper disclosure of their PII;
- f. loss of privacy;

- g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- h. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;
- i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;
- j. loss of use of and access to their account funds and costs associated with the 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 adverse credit notations; and,
- k. the loss of productivity and value of their time spent to address 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 such issues resulting from the Data Breach.

42. Even if Equifax has offered customers any meaningful credit monitoring or identity theft protection services for some level of future protection, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiffs and Class members, is ascertainable and is a determination appropriate for the trier of fact.

43. Equifax continues to hold PII of consumers, including Plaintiffs and Class members. Plaintiffs and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

### **CHOICE OF LAW**

44. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. residents against a company doing business in Georgia, has a greater interest in the claims of Plaintiffs and the Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

45. The principal place of business of Equifax, located at 1550 Peachtree Street NE, Atlanta, Georgia 30309, is the “nerve center” of its business activities – the place where its high-level officers direct, control, and coordinate the corporation’s activities, including its data security, and where: a) major policy, b) advertising, c) distribution, d) accounts receivable departments and e) financial and legal decisions originate.

46. Equifax’s response to, and corporate decisions surrounding such response to, the Data Breach were made from and in Georgia.

47. Equifax’s breach of its duty to customers, and Plaintiffs, emanated from Georgia.

48. Application of Georgia law to a nationwide Class with respect to Plaintiffs’ and the Class members’ claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

49. Further, under Georgia’s choice of law principles, which are applicable to this action, the common law of Georgia will apply to the common law claims of all Class members.



### **CLASS ALLEGATIONS**

50. Plaintiffs seeks 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), (b)(3) and (c)(4), Plaintiffs seeks certification of a Nationwide class defined as follows:

51. All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the “Nationwide Class”).

52. Excluded from each of the above Classes are Equifax and any of its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

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

54. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

55. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the

joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class include at least 143 million individuals whose PII was compromised in the Equifax Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

56. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

- a. Whether Equifax had a duty to protect PII;
- b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;
- c. Whether Equifax's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;
- d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

- e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;
- f. Whether Equifax's conduct constituted deceptive trade practices under Georgia law;
- g. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class members;
- h. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its POS systems and data network; and,
- i. Whether Plaintiffs and Class members are entitled to relief.

57. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their PII compromised in the Data Breach. Plaintiffs' damages and injuries are similar to other Class members and Plaintiffs seek relief consistent with the relief of the Class.

58. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Equifax to

obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

59. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. Instead, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

60. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

61. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Equifax failed to timely notify the public of the Breach;
- b. Whether Equifax owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;
- d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard the PII of Plaintiffs and the Class members; and,

f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

62. Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

## **COUNT I**

### **NEGLIGENCE**

#### **(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)**

63. Plaintiffs restate and reallege Paragraphs 1 through 62 as if fully set forth herein.

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

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

66. Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

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

67. Equifax also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather

PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

68. Equifax knew, or should have known, of the risks inherent in collecting and storing customer PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

69. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

70. Equifax breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class Members.

71. Since Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

72. Equifax had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Only Equifax had the ability to protect its systems and the PII it stored on them from attack.



73. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the data breach.

74. Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

- a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and 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 Class members' 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 and accurately disclose that Plaintiffs' and Class members' PII had been improperly acquired or accessed.

75. Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax possession or control.

76. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

77. Equifax breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members information regarding the breach until September 2017. Equifax has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

78. Through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

79. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately secure the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs

and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

80. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

81. Equifax's breach has caused Plaintiffs to suffer damages including, not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The

nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

## **COUNT II**

### **NEGLIGENCE PER SE (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)**

82. Plaintiffs restate and reallege Paragraphs 1 through 62 as if fully set forth herein.

83. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, the unfair act or practice by businesses of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax’s duty in this regard.

84. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Equifax’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax.

85. Equifax’s violation of Section 5 of the FTC Act constitutes negligence per se.

86. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

87. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

88. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the

far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

**COUNT III**

**WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT  
("FCRA")  
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)**

89. Plaintiffs restate and reallege Paragraphs 1 through 62 as if fully set forth here.

90. As individuals, Plaintiffs and Class member are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

91. Under the FCRA, a "consumer reporting agency" is defined 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).

92. Equifax 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.

93. As a consumer reporting agency, the FCRA requires Equifax 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).

94. Under the FCRA, a “consumer report” is defined as “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title.” 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information 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.

95. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, “and no other.” 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members’ PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

96. Equifax furnished the Nationwide Class members’ consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; 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.

97. 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.

98. Equifax 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. The willful and reckless nature of Equifax’s violations is supported by, among other things, former employees’ admissions that Equifax’s data security practices have deteriorated in recent years, and Equifax’s numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

99. Equifax also acted willfully and recklessly 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. Equifax 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 knowing of these legal obligations, Equifax acted consciously 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.

100. 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.

101. Plaintiffs and the Nationwide Class members have been damaged by Equifax's willful or reckless 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 . . . or damages of not less than \$100 and not more than \$1,000." 15 U.S.C. § 1681n(a)(1)(A).

102. 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 IV**

**NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT  
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)**

103. Plaintiffs restate and reallege Paragraphs 1 through 62 as if fully set forth herein.

104. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

105. Equifax's negligent conduct provided a means for hackers to obtain Plaintiffs' and the Class members' PII and consumer reports for no permissible purposes under the FCRA.

106. Plaintiffs and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the

Class members are entitled to recover “any actual damages sustained by the consumer.” 15 U.S.C. § 1681o(a)(1).

107. Plaintiffs and the 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 V**

#### **DECLARATORY JUDGMENT (ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)**

108. Plaintiffs restate and reallege Paragraphs 1 through 62 as if fully set forth herein.

109. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

110. Equifax still possesses PII pertaining to Plaintiffs and Class members.

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

112. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Equifax’s lax

approach towards data security has become public, the PII in its possession is more vulnerable than previously.

113. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

114. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures.

### **REQUEST FOR RELIEF**

**WHEREFORE**, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against EQUIFAX as follows:

- a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class;
- b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

- c. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;
- d. For an award of damages, as allowed by law in an amount to be determined;
- e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;
- f. For prejudgment interest on all amounts awarded; and
- g. Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMAND**

Plaintiffs demand a jury trial on all issues so triable.

Respectfully submitted, this 21<sup>st</sup> day of Septemer, 2017.

**CONLEY GRIGGS & PARTIN**

*/s/ Ranse M. Partin*

\_\_\_\_\_  
RANSE M. PARTIN

Georgia Bar No. 556260

4200 Northside Parkway, NW

Building One, Suite 300

Atlanta, GA 30327

Telephone: (404) 809-2591

Facsimile: (404) 467-1166

ranse@conleygriggs.com

**To Be Admitted Pro Hac Vice:**

**HEINS MILLS & OLSON, P.L.C.**

VINCENT J. ESADES  
310 Clifton Avenue  
Minneapolis, MN 55403  
Telephone: (612) 338-4605  
Facsimile: (612) 338-4692  
vesades@heinsmills.com

**KERKMAN WAGNER & DUNN**

K. SCOTT WAGNER  
839 North Jefferson Street Suite 400  
Milwaukee, WI 53202  
Telephone: (414) 277-8200  
Facsimile: (414) 277-0100  
swagner@kwdlaw.com

**PAVLACK LAW LLC**

ERIC PAVLACK  
225 North Alabama Street Suite 301  
Indianapolis, IN 46204  
Telephone: (317) 251-1100  
Facsimile: (317) 252-0352  
eric@pavlacklawfirm.com

**CENTO LAW, LLC**

G. JOHN. CENTO  
5915 North College Avenue Suite 100  
Indianapolis, IN 46220  
Telephone: (765) 280-3272  
cento@centolaw.com

**ATTORNEYS FOR PLAINTIFFS**

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)

KERI BAKKEN
GUSTAVO CARLO SANCHEZ

DEFENDANT(S)

EQUIFAX, INC.

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

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT (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)

Ranse M. Partin
CONLEY GRIGGS PARTIN LLP
4200 Northside Parkway, NW
Building One, Suite 300
Atlanta, GA 30327
(404) 467-1155
ranse@conlevgriggs.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION (PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF
2 U.S. GOVERNMENT DEFENDANT
3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
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)

Table with columns for PLF and DEF, and rows for citizenship categories: 1 CITIZEN OF THIS STATE, 2 CITIZEN OF ANOTHER STATE, 3 CITIZEN OR SUBJECT OF A FOREIGN COUNTRY, 4 INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE, 5 INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE, 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
7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT

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)

28 U.S.C. 1331 - diversity of citizenship.
This is a consumer data privacy class action seeking money damages.

(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



**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
- 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**

- 441 VOTING
- 442 EMPLOYMENT
- 443 HOUSING/ ACCOMMODATIONS
- 444 WELFARE
- 440 OTHER CIVIL RIGHTS
- 445 AMERICANS with DISABILITIES - Employment
- 446 AMERICANS with DISABILITIES - Other

**IMMIGRATION - "0" MONTHS DISCOVERY TRACK**

- 462 NATURALIZATION APPLICATION
- 463 HABEAS CORPUS- Alien Detainee
- 465 OTHER IMMIGRATION ACTIONS

**PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK**

- 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

**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**

- 610 AGRICULTURE
- 620 FOOD & DRUG
- 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- 630 LIQUOR LAWS
- 640 R.R. & TRUCK
- 650 AIRLINE REGS.
- 660 OCCUPATIONAL SAFETY / HEALTH
- 690 OTHER

**LABOR - "4" MONTHS DISCOVERY TRACK**

- 710 FAIR LABOR STANDARDS ACT
- 720 LABOR/MGMT. RELATIONS
- 730 LABOR/MGMT. REPORTING & DISCLOSURE ACT
- 740 RAILWAY LABOR ACT
- 790 OTHER LABOR LITIGATION
- 791 EEMPL. 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**

- 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
- 810 SELECTIVE SERVICE
- 875 CUSTOMER CHALLENGE 12 USC 3410
- 891 AGRICULTURAL ACTS
- 892 ECONOMIC STABILIZATION ACT
- 893 ENVIRONMENTAL MATTERS
- 894 ENERGY ALLOCATION ACT
- 895 FREEDOM OF INFORMATION ACT
- 900 APPEAL OF FEE DETERMINATION UNDER EQUAL ACCESS TO JUSTICE
- 950 CONSTITUTIONALITY OF STATE STATUTES
- 890 OTHER STATUTORY ACTIONS

**OTHER STATUTES - "8" MONTHS DISCOVERY TRACK**

- 410 ANTI TRUST
- 850 SECURITIES / COMMODITIES / EXCHANGE

**OTHER STATUTES - "0" MONTHS DISCOVERY TRACK**

- ARBITRATION (Confirm / Vacate / Order / Modify)

(Note: Mark underlying Nature of Suit as well)

**\* 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 \$ \_\_\_\_\_

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

**VIII. RELATED/REFILED CASE(S) IF ANY**

JUDGE Duffy 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/ Ranse M. Partin  
SIGNATURE OF ATTORNEY OF RECORD

9/21/2017  
DATE